Internet Users' Willingness to Disclose Biometric Data for Continuous Online Account Protection: An Empirical Investigation

Florian Dehling
Bonn-Rhein-Sieg University of Applied Sciences
florian.dehling@h-brs.de

Jan Tolsdorf
The George Washington University
jan.tolsdorf@gwu.edu

Hannes Federrath
University of Hamburg
hannes.federrath@uni-hamburg.de

Luigi Lo Iacono
Bonn-Rhein-Sieg University of Applied Sciences
luigi.loiacono@h-brs.de

ABSTRACT

Continuous authentication has emerged as a promising approach to increase user account security for online services. Unlike traditional authentication methods, continuous authentication provides ongoing security throughout the session, protecting against session takeover attacks due to illegitimate access. The effectiveness of continuous authentication systems relies on the continuous processing of users' sensitive biometric data. To balance security and privacy trade-offs, it's crucial to understand when users are willing to disclose biometric data for enhanced account security, addressing inevitable privacy concerns and user acceptance. To address this knowledge gap, we conducted an online study with 830 participants from the U.S., aiming to investigate user perceptions towards continuous authentication across different classes of online services. Our analysis identified four groups of biometric traits that directly reflect users' willingness to disclose them. Our findings demonstrate that willingness to disclose is influenced by both the specific biometric traits and the type of online service involved. User perceptions are strongly shaped by factors such as response efficacy, perceived privacy risks associated with the biometric traits, and concerns about the service providers' handling of such data. Our results emphasize the inadequacy of one-size-fits-all solutions and provide valuable insights for the design and implementation of continuous authentication systems.

KEYWORDS

Continuous Authentication, Biometric Traits, User Privacy Perception, Usable Privacy & Security, Factor Analysis, PLS-SEM

1 INTRODUCTION

Today, apps and online services generally establish authenticated sessions using entry point authentication only, such as during initial setup or when logging into a service. Usually, no additional verification of user authenticity occurs during these sessions. This means that, in practice, access to an app or online service is often linked to access to the device on which the session secret is stored in the ambient authority. Explicit re-authentication often only occurs for special actions, like financial transactions in online banking or changing a password. The duration of an authenticated session can vary, lasting for days, months, or until the user explicitly logs out, depending on the application context. In practice, this can lead to multiple authenticated sessions being available on a single device. If an attacker gains access to such a device, they not only have access to locally stored data but also to data accessible through apps and online services with active sessions. As a result, the security of these apps and online services is heavily dependent on the security of the device itself. Weak or non-existent device authentication therefore poses a risk to a wide range of services. Particularly in the mobile domain, users often use weak PINs or patterns for authentication, which an attacker can easily obtain through shoulder surfing, for example [5]. In addition, other factors such as purchasing used devices that were not properly reset before sale can also lead to unauthorized access to authenticated sessions [4]. For certain groups, particularly those facing political persecution, there is the risk of authorities compelling them to grant access to their devices and thus to all apps and online services with active authenticated sessions. By relying solely on entry point authentication, operators of these apps and online services lack the means to detect and prevent such unauthorized access to the services they provide. Even advanced entry point authentication mechanisms like Risk-Based Authentication (RBA) [96] do not allow verifying user authenticity throughout an entire session.

To address this shortcoming, recent developments in authentication mechanisms suggest that apps and online services themselves should continuously elicit and process hard-to-spoof biometric features throughout the entire session to ensure that the actual legitimate user is using the app or online service [3]. This mechanism is referred to as Continuous Authentication (CAuthN) [49]. It extends entry point authentication systems with continuous session authentication, promising improvements to security without invading the systems' usability due to additional authentication steps required by the users. In principle, CAuthN continuously assesses the risk of an authenticated user being an attacker. For this purpose, the literature proposes CAuthN systems which require the processing of various types of biometric traits [6, 18, 20, 33, 71, 82, 88].

The continuous processing of biometric data over the course of a session and all sessions during the usage lifetime of an app or online service makes CAuthN incredibly invasive. Respecting

Proceedings on Privacy Enhancing Technologies 2024(2), 479–508

https://doi.org/10.56553/popets-2024-0060

user privacy is of uttermost importance since it decides on user acceptance of a technology [61]. In addition, the processing of biometric data is subject to privacy laws, which require informing users about the processing and may even obtain users' consent. In this regard, research knows very little about users' privacy expectations towards CAuthN. In practice, developers are thus currently restricted to purely technical aspects when deciding on both the design of CAuthN and which biometric traits should be used. However, since privacy is highly context-dependent, it is hardly to be expected that users would accept the use of CAuthN and biometric traits equally for all services and apps. Due to the lack of insights on user privacy perceptions towards CAuthN, neither researchers nor developers have the knowledge to make well-founded design decisions beyond technical aspects. To deploy CAuthN in practice, understanding users' perceptions and privacy expectations is essential to design CAuthN solutions that respect user privacy, conform with obligations from privacy law, and are accepted by the users.

To investigate internet users' perspectives on CAuthN, we conducted a cross-sectional online survey with 830 participants from the U.S. between September and October 2022. Our research makes the following contributions: **(1)** We present the first comprehensive analysis of users' (privacy) risk beliefs, their trust beliefs, and their willingness to disclose biometric traits for the purpose of CAuthN. To incorporate contextuality, we used systematic manipulations in a between-subjects design to analyze user perceptions of seven different types of apps and online services commonly used in practice. **(2)** We provide the first empirical evidence that internet users distinguish between four groups of biometric traits with varying levels of willingness to disclose. **(3)** We provide evidence that context matters and that users' willingness to disclose for CAuthN varies for different types of apps and online services depending on the group of biometric traits. **(4)** We find that willingness to disclose is particularly high for biometric traits related to device interaction, whereas disclosure of biopotential traits (e.g., EEG) is rejected. **(5)** We find that users perceive the continuous disclosure of biometric traits as most acceptable for banking, payment, and cloud storage providers but least acceptable for social media, audio, and video streaming services. In this regard, users' willingness to continuously disclose individual biometric traits was positively influenced by users' beliefs that disclosure would help protect their accounts. In contrast, privacy risks perceived with the continuous disclosure and overall risk beliefs associated with processing such data by a service provider have mostly provable negative effects on willingness to disclose. **(6)** We found mostly no evidence for an effect on willingness to disclose for users' overall trust in a provider, their perceived risk for their account assets, and their expected vulnerability to becoming a victim of an attack. **(7)** Our results suggest that users would accept CAuthN independent of their awareness of potential attacks on their accounts and assets. Instead, acceptance of CAuthN appears to depend largely on beliefs about the efficacy of the measure and the risks to privacy posed by CAuthN.

Our research provides guidance to researchers and developers of CAuthN systems in deciding which biometric traits are most appropriate in terms of users' security and privacy perceptions in a specific application area. Our study results help to understand differences in user (privacy) perceptions and to respect special requirements for different application areas. In addition, our study helps understanding potential misconceptions and knowledge gaps regarding users' understanding of biometric traits.

The rest of this paper is structured as follows: first, we provide background information on CAuthN systems and summarize related work in Section 2. We then present our research model in Section 3 and our methodological approaches in Section 4. We discuss ethical considerations in Section 5. Our results are presented in Section 6 and discussed in Section 7. We highlight limitations and future work in Section 8 and conclude our paper in Section 9.

2 BACKGROUND

Below, we first provide a definition of biometric traits in Section 2.1. We then introduce the basics of CAuthN in Section 2.2 and discuss issues related to privacy law in Section 2.3. We then summarize related work on user perceptions of CAuthN in Section 2.4.

2.1 Biometric Data and Biometric Traits

In this study, we examine user perceptions of CAuthN systems that are based on the processing of biometric data, i.e., '*biological and behavioral characteristic[s] of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition*" (ISO/IEC 2382-37 [48]). Biometric recognition encompasses authentication scenarios such as biometric verification and identification. In CAuthN literature, the specific features are commonly referred to as biometric traits [94] and divided into *physiological* and *behavioral* traits. Examples of physiological traits include fingerprints, hand and face geometry, and retina. Examples of behavioral traits comprise hand signature, gait, keystroking, pointing, location, and brain wave. This separation aids in characterizing real-world biometric systems [15, 22, 32]. Although CAuthN is often linked to the use of behavioral biometric traits only, solutions exist that also continuously track physiological biometric traits [6, 18, 20, 33, 71, 82, 88]. We included both types of traits in our study to find out which type users would prefer in CAuthN.

2.2 Continuous Authentication Systems

Recently, technical aspects of CAuthN have been subject to an emerging number of publications in research on information security systems [1, 49, 88]. While the specific implementation of such systems varies, particularly in terms of the biometric data and features used, the underlying principle is mostly the same and is split into two phases [49]: (1) In the *enrollment phase*, the CAuthN system learns the legitimate state or behavior using biometric traits gathered from a user's interaction, e.g., by training a machine learning model. (2) After completing the training, CAuthN uses the trained model in the *authentication phase* to assess the biometric traits arising out of the current use of the service. When the biometric patterns observed during the authentication phase differ too much from the patterns observed in the training phase, the CAuthN system assumes illegitimate access and initiates countermeasures such as blocking access or asking for additional re-authentication.

In terms of implementation, CAuthN systems are often suggested in the context of mobile devices due to their rich sensor sets for collecting diverse biometric data [1]. Nevertheless, CAuthN systems are not restricted to a specific hardware environment and can also be deployed in Internet-of-Things scenarios [58] as well as in web

application scenarios [54]. Especially behavioral biometric data can be collected and processed in a platform-independent manner.

Biometric factors are crucial components of modern authentication systems. Their usage is currently focused on the unlocking of devices [9, 25, 92, 104]. Here, the primary objective is to enhance the usability of authentication by substituting the requirement of entering secrets, such as a password or PIN, with the disclosure of a biometric trait like a fingerprint [9]. In the context of entry point authentication systems, it is crucial to swiftly assess the authenticity of an access attempt using minimal biometric samples to make a highly accurate decision. In practice, fingerprint and facial recognition authentication methods are particularly prominent [9]. In contrast, CAuthN systems operate temporally after the initial entry point authentication and aim to ensure a user's authenticity throughout an authenticated session. To achieve this, biometric samples are continuously evaluated. This characteristic allows for incorporating additional biometric traits, particularly those falling within the realm of behavioral biometric data [82].

Whereas some work proposes that CAuthN systems replace traditional entry point authentication mechanisms like passwords [53], we consider such systems to be used as a complementary technology to strengthen account security. This is primarily due to the predominant machine learning-based detection algorithms, which are characterized by erroneous decisions, leading to the frequently used metrics False Acceptance Rate and False Rejection Rate [26]. To overcome these inaccuracies, the literature proposes using multimodal biometrics, i.e., mixing different types of biometric traits to increase the robustness of classification [82].

2.3 Legal Considerations

Because CAuthN requires the processing of biometric data, special legal considerations must be considered. In this regard, privacy bills recently signed in the U.S. as well as the General Data Protection Regulation (GDPR) [29] in the European Union (EU) classify biometric data as "*sensitive data*" (Colorado, Connecticut, Utah, Virginia), "*sensitive personal information*" (California), or "*special categories of personal data*" (EU). Such classification always implies stricter rules for the processing than is the case for non-sensitive personally identifiable information (PII). Apart from general privacy laws, several states in the U.S. have established specific biometric privacy acts or are planning to do so [66]. Well-known examples are the Illinois Biometric Information Privacy Act [46] and the Texas Capture or Use of Biometric Identifier Act [89], both of which have led to lawsuits against Facebook, Google, and TikTok [8, 42, 44, 77].

Regarding the use of biometric data, privacy bills in Colorado, Connecticut, and Virginia, as well as the GDPR in the EU, require making the processing of biometric data transparent and obtaining (explicit) consent from the individual. A composition of national and international supervisory data protection authorities in the EU has recently clarified that processing biometric data for identification purposes is generally subject to these requirements, too [28]. In addition, the GDPR requires conducting a privacy impact assessment. This process shall consider the perspectives of the data subjects, i.e., the perspectives of the individuals whose biometric data are processed (Article 35(9)). While it remains to be seen whether authorities in the U.S. will adopt this view, these decisions nonetheless have implications for private entities outside Europe, as rules of the GDPR apply even when data of individuals in the EU are processed outside the EU. Looking at U.S. and EU law, it is therefore likely that users must consent to the processing of their biometric data to be used for CAuthN. This highlights the importance of respecting users' privacy perceptions when deploying CAuthN.

2.4 User Perceptions

Existing studies and surveys on CAuthN have predominantly focused on technical aspects of feature processing and classification of various biometric traits [7]. To the best of our knowledge, empirical findings on user perceptions of CAuthN are scarce and highly fragmented. In an initial attempt, two studies conducted in the 1990s investigated user preferences for different types of biometric traits among 76 individuals from Australia [22] and 175 individuals in the UK [32]. Participants in these studies favored password authentication over biometrics in general, while also preferring single-time biometric authentication over continuous supervision. Exceptions were found for keystroke analysis and mouse dynamics, for which participants showed similar levels of acceptance across single-time and continuous authentication scenarios [32]. More recently, Rasnayaka and Sim [80] surveyed 494 mobile users' intention to adopt CAuthN in the context of eleven different mobile applications. They found that participants with lower security awareness had higher intention to adopt CAuthN and two-thirds of participants thought that CAuthN offers higher convenience and security. The study also revealed differences in users' security requirements for different mobile applications, but it disregarded correlations to users' willingness to use CAuthN. The study by Skalkos et al. [86] surveyed attitudes toward CAuthN of 778 users from the U.S. in a smartphone context. They found that privacy concerns had little to moderate effect on users' appraisals of the degree and likelihood of harm from the use of biometric systems. In addition, both perceived innovativeness and perceived response efficacy of CAuthN had moderate and strong significant effects on users' intention to use CAuthN. In a similar approach, Stylios et al. [87] surveyed attitudes towards CAuthN of 545 individuals from the EU, the U.S., and Canada. Participants were familiarized with common problems in authentication and with CAuthN as part of a seminar framed by a banking scenario. In conclusion, the study verified that perceived innovativeness, compatibility of CAuthN, and trust in technology had weak to moderate positive effects on users' adoption intention. Further, privacy concerns had strong effects on perceived risk, for which, however, no significant effects on adoption intention were found. Also, the study found no impact for perceived ease of use or perceived usefulness, revealing the need to treat biometrics separately in the context of CAuthN.

Results from previous studies on user perceptions specific to CAuthN are dated and suffer from insufficient contextualization of survey instruments. In particular, research conducted before 2000 [22, 32] reflects user perceptions of when biometrics were far less present than today. Furthermore, previous work either does not clearly define the application context [32, 80, 86, 87], the differentiation between single-time and continuous authentication [86], or the type of biometric trait used [80, 86, 87]. To the best of our knowledge, our study is the first to systematically investigate users'

perceptions across multiple types of biometric traits in different application contexts. We thereby clearly focus on using CAuthN to strengthen online account security. With our study design, we take particular care in contextualization, which has been proven to be critical in studying privacy issues [56, 78]. In conclusion, our study addresses previous studies' limitations and provides new insights necessary for studying and implementing CAuthN systems.

3 RESEARCH MODEL

In the following, we elaborate on existing research gaps and derive our research questions and hypotheses.

3.1 Differences in Willingness to Disclose

The successful deployment of CAuthN in online services depends on users' willingness to disclose biometric data. However, users' willingness to disclose PII is known to differ between different types of PII [69]. These differences often correlate with people's privacy and risk perceptions [75]. To convince internet users to consent to the processing of biometric data for CAuthN, it is therefore crucial to understand whether and which biometric traits internet users are willing to disclose for this purpose. Previous research on biometrics has mostly examined user perceptions of individual biometric traits in the context of specific systems and has focused on physiological biometric traits only [12, 13, 17, 36, 37, 52, 63, 74]. The studies did not compare users' perceptions of different types of biometric traits. Research including behavioral biometric traits only provides qualitative comparisons [32] and did not focus on CAuthN [22]. We address this research gap by answering the following research question:

RQ1a: Does internet users' willingness to disclose biometric traits for usage in CAuthN systems for online account protection differ between types of biometric traits?

The issue with studying differences in internet users' willingness to disclose individual biometric traits is that there are potentially many traits that cannot be examined in a single study. Privacy research addresses this issue by attempting to identify homogeneous groups of PII that reflect internet users' perceptions [47, 55, 72]. The benefit is that when new types of PII emerge, researchers and practitioners can use the groups as a guide to broadly classify them. We aim to provide similar utility for biometric traits and CAuthN, leading to our next research question:

RQ1b: Can different groups of biometric traits be identified which represent internet users' willingness to disclose biometric traits for usage in CAuthN systems for online account protection?

Privacy research showed that internet users' willingness to disclose is subject to contextual differences, i.e., users may be willing to disclose PII to online service X, but not to online service Y [56, 78]. In this regard, internet users may be willing to disclose biometric traits for use in CAuthN for specific types of online services, whereas they refuse disclosure for others. To study the influence of the online service type on internet users' willingness to disclose biometric traits, we formulate our next research question:

RQ1c: Does internet users' willingness to disclose biometric traits for usage in CAuthN systems for online account protection differ between types of online services?

3.2 Determinants of Willingness to Disclose

In addition to understanding differences in internet users' willingness to disclose biometric data for CAuthN, we also aim to understand its determinants, i.e., the factors related to or influencing internet users' willingness to disclose (cf. Fig. 1). Our objective is twofold: first, we aim to understand the effects of factors directly associated with specific types of biometric traits, as well as the effects of factors related to the type of online service. Second, we aim to understand the differences in determinants between different types of online services. This leads to the following research questions:

RQ2a: Which factors influence internet users' willingness to disclose biometric traits for CAuthN to strengthen online account security?

RQ2b: Are there differences in the factors' effects on internet users' willingness to disclose biometric traits for CAuthN to strengthen online account security across different types of online services?

As the number of determinants of users' willingness to disclose can be excessive, we limit our investigation to a set of factors derived from previous work, on which we then built a theoretical model. Basically, the model assumes that users' willingness to disclose a biometric trait is affected by (1) the gain of security due to CAuthN, (2) the loss of privacy due to the disclosure of the biometric trait, and (3) the context of an online service that is to be secured. Details of the model and our hypotheses are presented below.

Olt and Wagner [79] recently investigated the tension between the gain of security and the possible loss of privacy in the context of an online backup service. They combined the theory of goal-directed behavior [14] and the threat avoidance theory [65]. We adopted their results, indicating that the goal of security is represented by the impact of a security incident and its susceptibility. We thus hypothesize that the risk related to unauthorized access to an online account and its susceptibility promote users' willingness to disclose biometric traits for CAuthN:

H1a: A high level of a perceived risk that the asset secured by a private user account gets compromised due to unauthorized access has a positive effect on users' willingness to disclose biometric traits to be used in CAuthN.

H1b: A high level of susceptibility to unauthorized access on a user account leads to a positive effect on users' willingness to disclose biometric traits to be used in CAuthN.

In our study, we model a scenario where an online service provider processes the users' biometric traits to perform CAuthN. The online service provider thus is the recipient of the user's PII. Considering users' information privacy concerns, risk and trust related to the appropriateness of data handling must be respected, especially when comparing willingness to disclose between different online service types [68]. Previous work indicates that user acceptance of biometric passports depends on user trust in the technology and in the entities operating the technology [36]. Thus, we hypothesize that trust and risk related to the appropriate handling of biometric data disclosed for CAuthN affect users' willingness to disclose biometric traits:

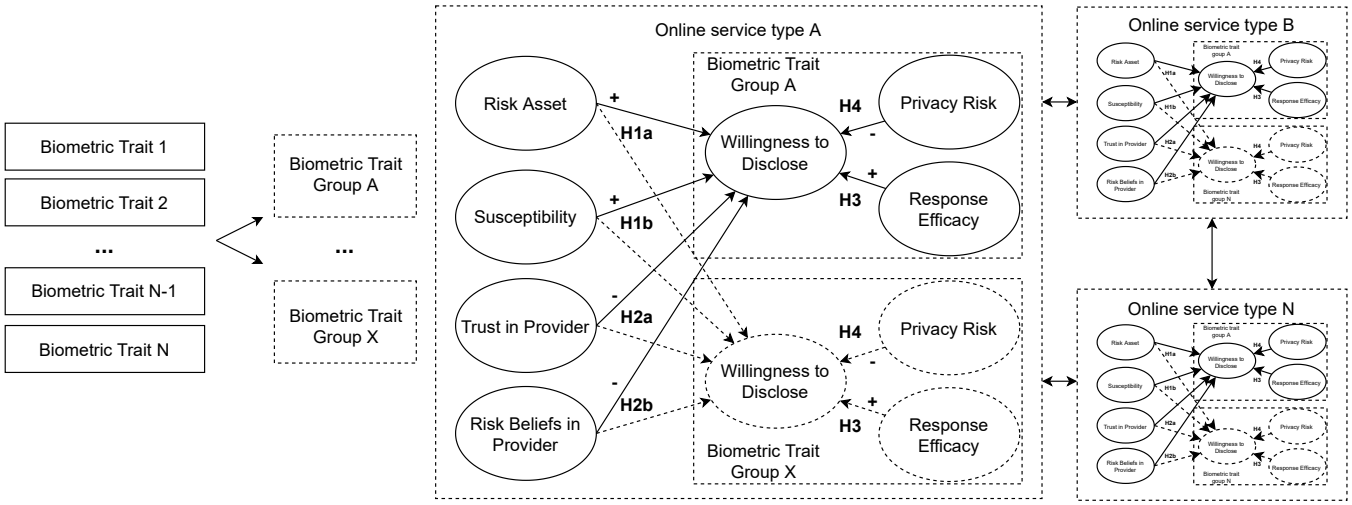


Figure 1: Structural model hypotheses and approach to analysis. (1) Identification of groups of biometric traits with shared latent factors on participants willingness to disclose. (2) Structural models (N=7) for each online service type with identified groups of traits as endogenous variables.

H2a: A high level of trust in the appropriate handling of biometric traits by an online service provider has a positive effect on users' willingness to disclose them.

H2b: A high level of risk related to the misuse of biometric traits by an online service provider has a negative effect on users' willingness to disclose them.

When it comes to coping with security threats, the perceived effectiveness of a mechanism plays an important role when users select mitigation strategies [79, 98]. Previous surveys showed that users' perceived usefulness is one of the strongest determinants of user attitudes towards biometric technology in general [37]. We thus assume that, besides weighing up security and privacy goals, the *response efficacy* of a given type of biometric trait influences users' willingness to disclose it for CAuthN:

H3: A high level of perceived response efficacy related to CAuthN using a given type of biometric trait has a positive effect on users' willingness to disclose it.

The willingness to disclose PII is affected by their sensitivity regarding users' privacy [91]. We thus hypothesize that the individual level of *perceived privacy risk* for a given type of biometric trait affects users' willingness to disclose:

H4: A high level of perceived risk for users' privacy related to a type of biometric trait has a negative effect on users' willingness to disclose this trait to be used in CAuthN.

4 METHODOLOGY

To examine our research questions and hypotheses, we conducted an online survey with 830 participants from the U.S. between September and October 2022. The data were analyzed quantitatively using appropriate statistical methods. In the following, we provide details on the study design and the measurement instruments.

4.1 Selection of Biometric Traits and Online Services

The scope of potential candidate biometric traits and online service types to study is inherently large. We thus focused on biometric traits whose suitability for CAuthN had already been studied. When selecting the online services, we took care to ensure that they were sufficiently diverse and used by a sufficiently large user group. Hence, our decisions to include or exclude biometric traits and online services were based on an iterative process. First, we extracted potential biometric traits from surveys on CAuthN and biometric authentication for information systems [6, 18, 20, 33, 71, 82, 88]. In a two-step approach, we first verified that the systems presented used the traits in a continuous manner and not as a replacement for entry-point authentication. We then grouped them according to the similarity of their sources, such as wrist and phone movements. The final list included 15 biometric traits and was used to assess users' willingness to disclose, response efficacy, and privacy risks in a between-group study design (cf. Table 1). This approach aimed to investigate how the characteristics of various online services or apps influence our participants' perceptions. In particular, we were interested in the impact of different levels of online service-specific perceptions regarding perceived security demands and appraisals regarding the handling of biometric data by a provider. In order to identify suitable online services, we assessed the usage frequencies of 13 types of online services in a screening study using a scale ranging "never," "less than monthly," "monthly," "weekly," and "daily". We excluded service types if fewer than 100 participants reported using them weekly or daily. We further analyzed the respondents' age and sex towards imbalance and excluded service types with significant accumulations. The final set of service types comprises Banking / Payment, Cloud Storage, Online Shopping, Messaging, Social Media, Video Streaming, and Music Streaming.

Table 1: Final selection of biometric traits and explanations provided to the participants.

Biometric Trait	Source	Explanation used in the survey
Keystroke Dynamics	[100]	The way you use a keyboard (e.g., how long you hold down a certain key).
Mouse Dynamics	[101]	The way you use a mouse (e.g., how long you hold down a mouse button or how fast you move the mouse pointer).
Touch Dynamics	[99]	The way you use a touchscreen (e.g., how lightly/strongly and how long you touch the screen).
Device Movement	[59]	Information on how your device moves while you use it.
Gait	[85]	Information on how your device (e.g., smartphone or smartwatch) moves as you walk or move.
Location Data	[85]	Information about your location, e.g., via GPS.
Connectivity Data	[35]	Information about what Wi-fi networks or Bluetooth devices are available in your surroundings.
Usage Profile	[54]	What functions of an application you use at what time.
Device Statistics	[76]	Hardware information of your device such as the energy consumption.
Fingerprint Recognition	[11]	Fingerprint sensor data.
Iris Recognition	[21]	Webcam images of your eyes.
Face Recognition	[19]	Webcam images of your face.
Voice Recognition	[27]	Audio data recorded with the microphone of your device.
Electroencephalogram (EEG)	[95]	Data from a sensor that monitors the activity of your brain.
Electrocardiogram (ECG)	[70]	Data from a sensor that monitors the activity of your heart (e.g., in a smartwatch).

4.2 Study Design and Procedure

We used a between-group design to compare user perceptions towards CAuthN for different types of online services, as it circumvents cross-over effects and keeps the workload to a minimum for our participants. We used a screening study to gather the full sample and elicit basic demographics. We also asked our participants to rate their usage frequency of different online services. Results from the screening study were used to split our sample into homogenous groups with respect to demographic variables. The usage frequency of online services was used to assign participants to a treatment condition, i.e., a specific type of online service. We thereby mapped participants to a service type they stated to use weekly to daily to avoid making the study seem too abstract to our participants.

In the main study (cf. Fig 2), we first contextualized our participants by asking them to provide up to three actions they usually perform with the online service type they were assigned to. We then asked them to rate the risk of an unauthorized entity accessing their online service account and the susceptibility of such an incident. In the next step, participants were introduced to CAuthN and biometric traits by watching a short explanation video on CAuthN. The video explained the risk of an authenticated session takeover in a scenario where an attacker gets unauthorized access to an online account through gaining access to a device holding an authenticated session. CAuthN performed by the online service provider was proposed as mitigation. The rationale for choosing this scenario is twofold. Primarily, it enables the study of user perceptions in relation to the novel key features of CAuthN systems, in particular the additional security provided by the continuous protection of the authenticity of an active session that has already been authenticated. Second, by choosing a scenario where the biometric traits are disclosed to the online service or app provider to perform CAuthN, we wanted to ensure that our results were not influenced by the technical knowledge of our participants. Previous research has shown that new security mechanisms can be susceptible to misunderstandings that can affect how participants evaluate the privacy and security of a system [62]. We therefore reduced complexity by choosing a worst-case scenario. However, we would point out that alternative and privacy-enhancing approaches to CAuthN are feasible, in which biometric data is processed primarily or entirely locally on the client device.

We adopted the explanation videos to the specific online service types by naming them in the voiceover and accompanying text and by using logos of popular example services. After the video, participants had to solve a quiz comprising five questions on the idea of CAuthN. They were allowed to watch the video again if necessary. After the quiz, participants were shown if they answered correctly. In case of an incorrect answer, we provided them with the correct solutions and additional explanations.

After familiarizing the participants with the context of the online service type and the concepts of CAuthN and biometric traits, we asked them to rate their *willingness to disclose*, *perceived response efficacy*, and *loss of privacy due to disclosure* to the service provider for each of the biometric traits. We provided short descriptions (cf. Table 1) and icons. Afterward, participants were asked about the risk and trust related to the appropriate handling of biometric data by the online service provider. The survey closed with questions about general security attitudes and information privacy concerns.

To design our study, we used established measurement instruments from the literature and adapted them to our needs (cf. Table 2). We used items from [50, 68] to assess $\text{Risk}_{\text{Asset}}$, $\text{Susceptibility}_{\text{Asset}}$, $\text{Trust}_{\text{Provider}}$, and $\text{Risk}_{\text{Provider}}$. Items for $\text{Risk}_{\text{Asset}}$, $\text{Trust}_{\text{Provider}}$, and $\text{Risk}_{\text{Provider}}$ were measured on a seven-point scale. $\text{Susceptibility}_{\text{Asset}}$ was measured on a 5-point scale. Willingness to Disclose, Response Efficacy, and Privacy Risk were measured individually for each type of biometric trait using sliders in the range of zero to 100. We further included the scale Self-Report Measure of End-User Security Attitudes (SA-6) [30], and the scale Internet Users' Information Privacy Concerns (IUIPC) [68]. Instead of using the original IUIPC-10, we used the IUIPC-8 with two items removed due to its better factorial validity and reliability [34]. SA-6 was measured on a 5-point scale and IUIPC-8 on a 7-point scale, respectively. For each service type, we adapted the questions, items, and explanations used by

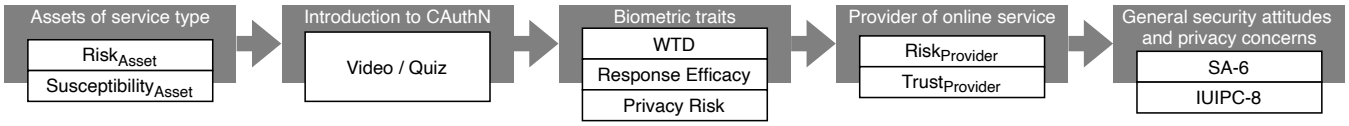


Figure 2: Schematic overview of the main survey flow with thematic groups and constructs elicited.

substituting the service type only. For example, instead of *"your favorite cloud storage website or mobile app"* we used *"your favorite banking & payment website or mobile app."*

We decided not to limit the scenario in our study to a specific device type used to let participants assume their usual usage behavior (mobile or not) and not to limit the types of biometric traits as it would not be appropriate to assess, e.g., mouse dynamics in a mobile-only study. We follow results from [83], indicating that users' usage behavior regarding tasks to accomplish or security concerns did not significantly differ between mobile and laptop use.

Our study design, all texts, and the questions and items in our surveys were reviewed by other researchers in our institution who have expertise in topics on RBA, CAuthN, and conducting online surveys. Furthermore, the content was revised by a native speaker from the U.S. to ensure that the explanations and questions make sense to the target population, i.e., internet users from the U.S. In addition, we conducted a pilot study with 30 participants to test our survey and improved descriptions and presentation. An outline of the final questionnaire is available in Appendix A.

Table 2: Constructs used in the survey and their definitions.

Construct	Definition
Willingness to Disclose	Willingness to continuously share biometric trait t with a website or mobile app of type s to improve account protection.
Response Efficacy	Belief that continuously sharing biometric trait t with a website or mobile app of type s improves account protection [50].
Privacy Risk	Perceived privacy risk when continuously sharing biometric trait t with a website or mobile app of type s to improve account protection.
$\text{Risk}_{\text{Asset}}$	Risk beliefs associated with someone getting unauthorized access to an account at a website or mobile app of type s [68].
$\text{Susceptibility}_{\text{Asset}}$	Probability of someone getting unauthorized access to an account at a website or mobile app of type s [50].
$\text{Trust}_{\text{Provider}}$	The degree to which participants belief the provider of a website or mobile app of type s is dependable in protecting their biometric trait t [68]
$\text{Risk}_{\text{Provider}}$	The expectation that a high potential for loss is associated with the release of biometric trait t to the provider of a website or mobile app of type s [68].

4.3 Participant Recruitment

We recruited our participants via the online panel Prolific. The panel allowed us to include screening filters for internet users located in the U.S. and to obtain a sample balanced by participant sex. If participants in our screening study agreed to participate in our main study, we re-invited them using a pseudonymous user identifier provided by the Prolific platform. In total, 1219 participants participated in our main study. To clean our data, we removed participants who failed attention checks or did not provide an answer for the biometric trait-related items WTD, Privacy Risk, and Response Efficacy. We further decided to exclude participants who failed to give the correct answers to the quiz about CAuthN. By doing so, we aimed to ensure that all participants in the analyses understood the principle of CAuthN as a technology that can improve their account security. The final dataset consists of 830 participants across seven study conditions (cf. Table 3 for distribution). The response time for valid surveys averaged 14.1 minutes (median = 12.5 minutes).

Table 3: Distribution of participants across study conditions with different online service types.

Study Condition	n	Study Condition	n
Banking / Payment	115	Social Media	130
Cloud Storage	115	Video Streaming	123
Online Shopping	134	Music Streaming	107
Messaging	106		

5 ETHICAL AND LEGAL CONSIDERATIONS

Our institution is in the EU and has no formal IRB process. However, we followed the strict rules of our national and European privacy regulations. Our study was reviewed and approved by our institution's data protection officer. We used pseudonymous user-IDs provided by the recruiting platform to map participants between the pre-screening and the main study. The user-IDs do not allow for direct identification. We informed our participants about the data collected at the beginning of both survey parts and asked them for informed consent. Each question included a "prefer not to answer" option. Respecting the minimum wage in the U.S. at the time of the study, participants were paid 15$ per hour adjusted to the median completion time of the study condition attended. Participants' data were stored and backed up on encrypted hard drives only.

6 RESULTS

In this section, we present the results and describe the analyses performed. Except for the structural equation modeling, all analyses were performed with R v4.2.1. Structural equation modeling was done with SmartPLS 4.

6.1 Demographics

Our participants' demographics are summarized in Table 4. A summary of all subsamples is available in the Appendix (cf. Table 6). Overall, our sample is balanced by female and male participants. Half of our participants were between 28 and 46 years old ($mean$ = 38.2, sd = 13.2). Our sample is characterized by white ethnicity and high levels of education, with 55% having an undergraduate degree or higher. We used chi-square tests of homogeneity to identify significant differences in demographic distributions across the treatment groups. Except for employment status (χ^2 (36, n = 830) = 55.9, p = .017), we could reject the hypothesis of proportions being different across the study conditions. Considering effects of privacy concerns or security attitudes, we also tested for proportional differences in the ratings for IUIPC-8 and SA-6. A chi-square test on both constructs showed no significant differences (IUIPC-8: χ^2 (168, n = 830) = 164.12, p = .57; SA-6: χ^2 (138, n = 830) = 124.87, p = .781). Our participant's SA-6 score averaged 21.07 (sd = 4.67, $median$ = 22, max = 42), and the mean IUIPC-8 score was 48.75 (sd = 6.02, $median$ = 50, max = 56), indicating a medium level of security attitudes but a high level of information privacy concerns.

Table 4: Participant demographics summary (n = 830).

Sex	%
Female	50.1
Male	49.9
Age	%
18-24	13.7
25-34	34.2
35-44	24.3
45-54	12.8
55-64	10.0
>65	4.9
Ethnicity	%
Asian	5.5
Black	3.5
Mixed	6.1
Other	1.8
White	83.0
Employment Status	%
Full-Time	46.6
Part-Time	18.1
Homemaker/ Retired or Disabled	15.3
Unemployed	13.1
Other	6.9

Annual Household Income	%
<10k	6.9
10k-20k	8.3
20k-40k	18.4
40k-60k	16.7
60k-80k	17.0
80k-100k	10.6
100k–150k	13.4
>150k	8.7
Relationship Status	%
Partnership	54.0
Single	43.6
Highest Education Level	%
Doctorate degree	2.8
Graduate degree	12.7
Undergraduate degree	39.6
High school diploma/ A-levels	26.4
Secondary education	2.3
Technical/ Community college	15.4

Note. NAs are omitted

6.2 Characteristics of Online Service Types

We used the between-group study conditions to frame participants with different levels of $\mathbf{Risk_{Asset}}$, $\mathbf{Risk_{Provider}}$, and $\mathbf{Trust_{Provider}}$. For analysis, we first checked for significant differences between online service types using a Kruskal-Wallis rank sum test and examined the effect size [43, 90]. Running a Dunn's test with Bonferroni correction for pairwise comparison revealed significant differences between the between-group conditions (cf. Fig. 3, details in Appendix Table 7) [23]. We chose robust statistical tools to respect the non-normality of our participant's ratings.

The risk associated with unauthorized access to an account ($Risk_{Asset}$) was rated highest for Banking / Payment and Online Shopping, followed by Messaging, Cloud Storage, and Social Media. $Risk_{Asset}$ for Video and Music Streaming was ranked lowest. A pairwise comparison revealed significant differences ($p < .05$) except between Banking / Payment and Online Shopping; Cloud Storage and Messaging; Online Shopping and Social Media; Messaging and Social Media; and Music Streaming and Video Streaming (cf. Appendix Table 8).

Participants' perceived risk related to the provider's unappropriated handling of biometric traits ($Risk_{Provider}$) was significantly lower for Banking / Payment and Cloud Storage than for Messaging, Social Media, Music- and Video Streaming ($p < .05$). In contrast, we found significantly higher ratings of trust in the appropriate handling of data ($Trust_{Provider}$) for Banking / Payment and Cloud Storage than for Messaging, Social Media, and Video Streaming ($p < .05$).

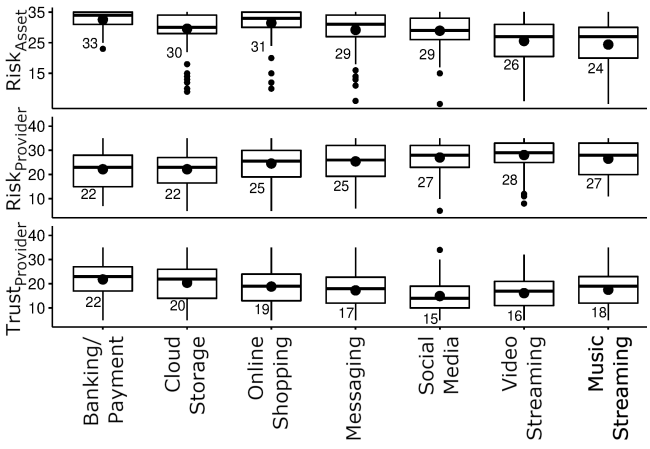


Figure 3: Participants' ratings for $\mathbf{Risk_{Asset}}$ (top), $\mathbf{Risk_{Provider}}$ (middle), and $\mathbf{Trust_{Provider}}$ (bottom) across online service types. Numbers correspond to the mean.

6.3 Factorial Analysis of Willingness to Disclose Biometric Traits

Analyzing the results for 15 types of biometric traits in seven online service types can lead to rather complex results with low practical meanings. In preparation for answering **RQ1b**, we decided to first identify groups of biometric traits with similar user perceptions. Since we expect our participants' ratings for WTD to depend on

the context of an online service type and thus differ between study conditions, a global clustering would not be appropriate. Clustering the ratings separated by each online service type would respect our assumptions, however, it would limit the explanatory value and the practical use, especially if the clusters differ between online service types. We chose an Exploratory Factor Analysis (EFA) combined with an Confirmatory Factor Analysis (CFA) [38] applied to participants' ratings for willingness to disclose (WTD) since we expect groups of biometric traits to be assessed similarly by users due to an underlying latent factor originating from the characteristics of the biometric traits in question. We split our sample in to half to identify the latent factors with the EFA, and to validate our results using the CFA based on independent subsamples. We verified that both subsamples (N_{EFA} = 417, N_{CFA} = 413) had non-significant differences in demographics, IUIPC-8, and SA-6 scores. We followed guidelines by Hair et al. [38] and Zygmont and Smith [105] to set up and analyze both the EFA and CFA. To perform the EFA, we first assessed and confirmed the factorability using the Kaiser–Meyer–Olkin criterion (KMO = .916) and Bartlett's test of sphericity ($\chi^2(91) = 4916.076$, $p < .001$) [24]. To approximate the number of factors to be extracted, we used a parallel analysis, the Root Mean Square Error of Approximation (RMSEA), as well as the Akaike Information Criterion (AIC) and the Bayesian Information Criterion (BIC) [41]. The factor retention criteriums suggested extracting between 4 and 5 factors. We fitted models using the EFA dataset and used Promax as an oblique factor rotation, since we expected that users' willingness to disclose a specific type of biometric trait correlates with a user's overall "latent" willingness to disclose biometric data. Due to the mostly skewed data, we used an Ordinary Least Squares (OLS) factor analysis [105]. Since using five factors did not lead to relevant loadings on all factors, we continued iteratively refining the model using four factors. To confirm the factors identified with the EFA, we ran a CFA on the second subsample using a robust maximum likelihood estimator to account for outliers and non-normal distribution of the data. The model fit indices show a good model fit, and the indicators for construct reliability support the assumption that the factors found can be considered resilient (cf. Table 5). We interpreted the results of EFA and CFA and labeled the latent factors influencing users' willingness to disclose different types of biometric traits as follows:

Device Interaction Behavioral Traits With loadings on Mouse Dynamics, Keystroke Dynamics, Touch Dynamics, and Device Movement, this factor describes behavioral biometric traits resulting from users' physical interaction with a device. The EFA additionally considers Gait as an indicator but with a rather low loading (λ = .4), which is why we decided to exclude this trait from further analysis. Our participants' rated the Device Interaction traits with a low level of privacy risk and a medium level of response efficacy.

Body-Related Physiological Traits All related to physiological characteristics of an individual, Face, Iris, Fingerprint, and Voice Recognition are classical traits known as physiological biometric traits. The Body-Related group was assessed with the highest rating for privacy risk and the highest level of response efficacy.

Profiling-Related Behavioral Traits The third factor identified groups of behavioral biometric traits resulting from users' interaction with apps and services. The biometrics grouped under this factor include general Profiling of usage patterns, Connection Data, Device Statistics, and Location Data. Different from the factor Device Interaction, this group of behavioral biometric traits is less related to an active interaction with hardware but with data originating from apps running on the device. Profiling-Related traits were rated with a medium response efficacy and a medium to high level of privacy risk.

Biopotential Physiological traits The two biometric traits EEG and ECG are suggested to be an additional factor. Even though they are related to the human body, the CFA clearly separates them from the factor Body-Related traits. Since this factor only consists of two indicating variables with strong correlation (r = .8), we excluded it from our structural model described in Section 6.6. The traits in this group were rated with the lowest level of response efficacy observed and have been assessed with a medium to high level of privacy risk.

Regarding **RQ1b**, we conclude that biometric traits can be grouped according to internet users' willingness to disclose. Our results suggest that users differentiate between four broad types of biometric traits: (1) Device Interaction, (2) Body-Related, (3) Profiling-Related, and (4) Biopotential.

Table 5: Results Confirmatory Factor Analysis.

Model fit			
χ(df), ***: p <.001	(71): 180.45 ***		
CFI	.96		
SRMR	.048		
RMSEA	.061		
Recommended values [38]: CFI >.92, SRMR ≤ .08, RMSEA <.07			
Identified latent constructs			
Device Interaction Behavioral Traits	λ	α	.94
Touch Dynamics	1	ω	.94
Keystroke Dynamics	.99	AVE	.81
Mouse Dynamics	1		
Device Movement	.88		
Profiling-Related Behavioral Traits	λ	α	.84
Connectivity Data	1	ω	.85
Device Statistics	.99	AVE	.58
Usage Profiling	.87		
Location Data	.85		
Body-Related Physiological Traits	λ	α	.89
Iris Recognition	1	ω	.89
Face Recognition	1	AVE	.68
Voice Recognition	.84		
Fingerprint Recognition	.95		
Biopotential Physiological traits	λ		
EEG	1		
ECG	1.2		
Recommended values [38]: $\lambda \geq .7$, $\alpha \geq .7$, $\omega \geq .7$, AVE ≥ .5			

6.4 Intra-Service Differences in Willingness to Disclose (WTD)

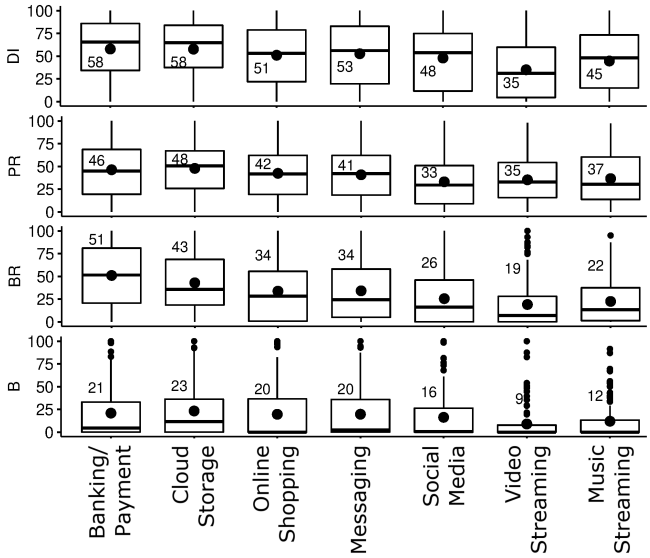
To study differences in willingness to disclose biometric traits under **RQ1a**, we compared the mean average scores for each group of biometric traits identified in the previous step (cf. Fig. 4, details in Appendix Table 9). To respect contextual differences between conditions, we conducted seven within-group comparisons, one for each online service type. We chose robust methods since participants' ratings resulted in mostly skewed data from partially extreme high or low ratings. The comparison of means was conducted by computing robust one-way repeated measures ANOVA for trimmed means and resulted in significant differences for all survey conditions. A Yuen's test for trimmed means [2] showed small to large effects. The corresponding post-hoc tests for pairwise comparisons [97] showed significant differences for most groups of biometric traits as outlined in the following (cf. Appendix Tables 10-16).

Except for the Banking / Payment condition, the overall ranking of WTD was Device Interaction, Profiling-Related, Body-Related, and Biopotential, with the latter having the lowest ratings (c.f. Fig. 4). In the Banking / Payment condition, participants' WTD for Body-Related traits was remarkably high, resulting in no significant differences to Device Interaction and Profiling-Related traits. The pairwise comparisons for the remaining study conditions showed significant results except for Body-Related and Profiling-Related in Messaging, as well as for Device Interaction and Profiling-Related in Video Streaming. The latter was caused by a noticeably low rating for Device Interaction biometrics for Video Streaming.

Regarding **RQ1a**, we conclude that internet users' willingness to disclose biometric traits for CAuthN differs depending on the type of trait used. Our results suggest that for most online service types, users prefer Device Interaction biometrics over Body-Related and Profiling-Related ones. Using Biopotential traits is predominantly rejected.

6.5 Biometric Traits in Different Contexts

We examined the ratings for groups of traits between study conditions to investigate differences in willingness to disclose biometric traits between different service types (cf. Appendix Table 17). To respect the skewed data for WTD, we used Kruskal-Wallis rank sum test and Dunn's test with Bonferroni correction for pairwise comparison as corresponding post-hoc analysis applied on the mean average scores for each group of biometric traits [23, 43]. A pairwise comparison of **Device Interaction** biometrics across the study conditions revealed that for Video Streaming, the willingness to disclose these types of biometric traits was significantly lower than for all other online service types except for Music Streaming. **Profiling-Related** traits were rated lowest for Social Media. We found significant differences compared to Banking and Cloud Storage. The latter received the highest ratings for all service types, which was, besides Social Media, also significantly higher than for Video Streaming. The **Biopotential** traits received low ratings for all study conditions. Nevertheless, there were differences between both Banking / Payment and Cloud Storage and Video Streaming, with lower ratings for the latter. Also, willingness to disclose was significantly lower for Music Streaming than for Cloud Storage. Willingness to disclose **Body-Related** traits was significantly higher for Banking / Payment than for all other online service types except Cloud Storage. For Cloud Storage, the pairwise comparison showed significantly higher ratings than for Music- and Video Streaming and Social Media. Video Streaming was rated lowest and significantly lower than Online Shopping and Messaging.



DI: Device Interaction, PR: Profiling-Related, BR: Body-Related, B: Biopotential. Numbers correspond to the mean.

Figure 4: Participants' ratings of willingness to disclose groups of biometric traits in different study conditions.

Even though an absence of significance is no proof of equality, the small effect sizes for Profiling Related ($\eta^2 = .024$) and Biopotential traits ($\eta^2 = .023$) indicate a rather low impact of service types on users' willingness to disclose those types of traits. The significantly low ratings for Device Interaction traits in the Video Streaming condition result in a bigger but still "small" effect ($\eta^2 = .043$) [16]. The high ratings for Body-Related traits in the Banking / Payment and Cloud Storage condition lead to a moderate effect size ($\eta^2 = .093$) and show that the context of use must not be disregarded without differentiating the type of biometric trait.

Regarding **RQ1c**, we conclude that internet users' willingness to disclose biometric traits for CAuthN depends on the context of the online service type.

6.6 Structural Model of Willingness to Disclose

We used Partial Least Squares based Structural Equation Modeling (PLS-SEM) to explore factors influencing users' willingness to disclose biometric traits for CAuthN (**RQ2a**). We chose PLS-SEM over Covariance-based Structural Equation Modeling (CB-SEM) because we aimed to test our hypothetical framework, consisting of 13 constructs that originate from data with a lack of normality (cf. Fig. 1). Each model has three endogenous variables, i.e., WTD

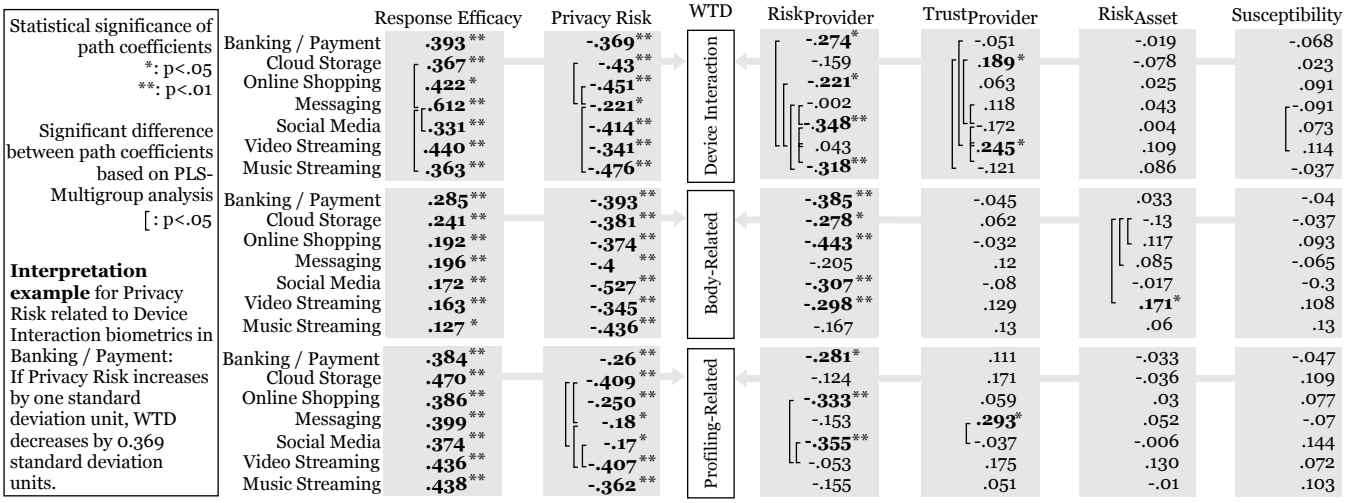


Figure 5: Path coefficients of PLS-SEM for groups of biometric traits across all online service types.

Body-Related, WTD Profiling-Related, and WTD Device Interaction. Each WTD is connected with its corresponding privacy and response efficacy. Additional determinants modeled were the online service type specific $\text{Risk}_{\text{Asset}}$, $\text{Susceptibility}_{\text{Asset}}$, $\text{Risk}_{\text{Provider}}$, and $\text{Trust}_{\text{Provider}}$. Since one measurement model references a single online service type, we ran seven models to examine contextual influences using a multigroup analysis for answering **RQ2b**.

We assessed the measurement models and resulting structural models following guidelines by Hair et al. [39]. Overall, the seven measurement models showed reflective indicator loadings > .7, indicating acceptable item reliability. Few exceptions with weaker loadings were found for measurement models in all conditions, but we still deemed the constructs acceptable because we could not identify patterns across all conditions. Internal consistency reliability ρ_α of four measurement models was between Cronbach's Alpha as the lower bound and the composite reliability as the upper bound, indicating sufficient construct reliability. Three models had constructs with ρ_α outside the recommended bounds ($\text{Susceptibility}_{\text{Asset}}$ in Music Streaming and $\text{Risk}_{\text{Asset}}$ in Banking / Payment and Social Media), indicating limited composite reliability for the constructs affected. Convergent validity of the measurement constructs showed an appropriate average variance extracted (AVE > .5) except for $\text{Risk}_{\text{Asset}}$ in the Banking / Payment and the Social Media model. Discriminant validity was confirmed since the Heterotrait-Monotrait (HTMT) ratio of the correlations was < .85, except for one outlier of .87 for two conceptually similar constructs. The Variance Inflation Factor (VIF) for all predictor constructs was lower than 3.33 indicating no collinearity issues. R^2 values for the endogenous constructs were in the range [.4, .7] and attested to the models' moderate to substantial explanatory power. The endogenous constructs' Q^2 values were in the range [.3, .6] and can be rated as medium to large predictive accuracy. PLSpredict-based assessment of the models' predictive power resulted in Q^2_{predict} values >0, and a higher error rate in terms of RMSE for the linear regression model than for the PLS-SEM in all cases and thus showed a high predictive power. To test our hypotheses, we assessed the structural models' path coefficients and their p-values resulting from a bootstrapping with 5000 subsamples (cf. Fig. 5, details in Appendix Tables 18 - 24).

For $\text{Risk}_{\text{Asset}}$, we only found one significant path pointing to the WTD of Body-Related traits in Video Streaming. Since the coefficient is rather low (.17), we reject our hypothesis H1a and conclude that for our sample, the risk related to unauthorized access to an account does not play a major role when deciding to disclose biometric traits. Since the results do not show a significant path coefficient for the influence of $\text{Susceptibility}_{\text{Asset}}$ on the WTD at all, we also have to reject our hypothesis H1b. The influences of risk and trust related to the appropriate handling of biometric traits by the provider are diverse, especially between the service types. While $\text{Trust}_{\text{Provider}}$ had a significant positive effect on the WTD, $\text{Risk}_{\text{Provider}}$ showed a negative effect. For $\text{Trust}_{\text{Provider}}$, we only found significant paths to Device Interaction biometrics in the Cloud Storage and Video Streaming conditions, as well as for Profiling-Related traits in Messaging. We, therefore, could only partially confirm hypothesis H2a. The amount of significant paths increases for $\text{Risk}_{\text{Provider}}$. We found significant paths for all groups of biometric traits in the conditions of Banking / Payment, Online Shopping, and Social Media. Since there are combinations of groups of traits and online service types with no significant paths between $\text{Risk}_{\text{Provider}}$ and WTD, we could, again, only partially confirm hypothesis H2b. We identified significant paths for response efficacy and privacy risk in all groups of traits across all study conditions and thus could fully confirm hypotheses H3 and H4. While response efficacy promoted our participants' WTD, the perceived risk for participants' privacy showed a negative effect.

Regarding **RQ2a** and **RQ2b**, we identified different factors influencing internet users' willingness to disclose depending on the online service type. Overall, we find no evidence that users' perceived susceptibility and risk associated with the asset of an online service type, nor trust in the provider, have a significant effect on users' willingness to disclose biometric traits for CAuthN. Yet, we find partial evidence that users' perceived risk associated

with inappropriate handling of biometric data by the provider has a significant effect on their willingness to disclose. Its effect varies between online service types as well as between groups of biometric traits. Moreover, we find evidence that privacy risks and response efficacy have weak to moderate effects on participants' willingness to disclose biometric data for CAuthN.

7 DISCUSSION

To answer our research questions under **RQ1**, we examined internet users' willingness to disclose biometric data for CAuthN. Indeed, we find that willingness to disclose differs significantly among different types of biometric traits (**RQ1a**). Based on empirical evidence, our results suggest that internet users differentiate between four groups of biometric traits (**RQ1b**). In this regard, we find that in most online service contexts, participants preferred Device Interaction traits to be used over Body-Related and Profiling-Related ones but rejected the use of Biopotential traits. Furthermore, we showed that participants' willingness to disclose those groups of traits depends on the online service context (**RQ1c**). Especially, we find that users' willingness to disclose Body Related traits is higher in the Banking / Payment and Cloud Storage conditions compared to other contexts. Our findings have important implications for research and practice, as it shows that previous studies that survey individual biometric traits or simply ask questions such as "Are you willing to disclose biometric data?" compromise generalizability and validity. The varying perceptions of biometric traits in different use cases highlight the importance of contextualizing study settings. For instance, results obtained in the context of an online banking scenario (e.g., [87]) cannot be readily extrapolated to other use cases. In addition, instead of comparing individual biometric traits like previous research [32], the identified groups allow for more generic conclusions. Based on inspection, the four groups still apply to previous research findings and allow for categorizing future biometric traits, which are not yet available. Consequently, we are confident that the results of our study enable a user-centric impact assessment of various types of CAuthN systems. Especially, the observed differences in willingness to disclose different types of biometric traits have implications for users' acceptance of a particular CAuthN system. For instance, it can be assumed that the use of Body-Related biometrics in contexts such as social media or online shopping would be perceived as inappropriate. In the case of multimodal CAuthN systems [82], i.e., a system combining different biometric traits, our findings become particularly relevant. For example, when combining keystroke dynamics (Device Interaction) and face recognition (Body-Related) [84], users are likely to evaluate the overall system based on the biometric trait they perceive as most privacy-invasive. To ensure high acceptance, multimodal systems could combine features solely from the same group, e.g., either Device Interaction or Body-Related. In such a case, our findings help select the most appropriate group of biometric traits according to the context of an application while respecting users' (privacy) preferences.

Regarding our research questions under **RQ2** and our hypotheses **H1-H4**, we examined which factors influence our participants' willingness to disclose biometric traits for CAuthN systems. We found no evidence that participants' perceived risk associated with unauthorized access to their account has an effect on their willingness to disclose. Likewise, we find no evidence for perceived susceptibility either. Rather, our results suggest that subjects weigh the perceived efficacy of a biometric trait against the loss of privacy associated with disclosing biometric data for CAuthN.

Our survey instrument does not allow us to make statements about the reasons why participants perceive a loss of privacy when providing biometric data to the operator of an app or online service for CAuthN. However, in essence, the disclosure of biometric data entails a loss of control over them. This can lead to various privacy risks for the self-disclosing subject. For instance, data may unintentionally leak due to a security breach, government authorities may gain access through legal regulations, or unscrupulous service providers may intentionally share or sell the data illegally. The identified groups of biometric traits not only differ in their willingness to disclose but also in the potential privacy risks associated with disclosure or misuse. Body-Related traits, such as fingerprints, are characterized by their immutability [81]. Losing control over such data can have far-reaching consequences, as biometric systems are used in various aspects of life, such as border control [60]. Biopotential traits fall under the category of health data. Potential privacy risks here can be quite diverse. For instance, EEG data can reveal not only information about age and gender but also neurological conditions or medication usage [45]. Profiling-Related traits are already used in web tracking for user analysis or the provision of specific services, allowing inferences about an individual's life circumstances [10, 57, 64]. In contrast, traits from the Device Interaction group have limited information content but still enable the recognition of a person based on their behavior [40]. The averaged assessment of the loss of privacy when disclosing different groups of biometric traits shows a consistent ranking across all service types (cf. Appendix Table 9). Respondents perceive the highest loss of privacy with Body-Related traits, followed by Biopotential traits, Profiling Related traits, and Device-Interaction traits. Biometric traits directly linked to the physical identity of the respondents are generally considered more sensitive. It remains uncertain whether our participants were truly aware of the specific privacy risks, as, for example, the analysis possibilities of EEG data as representatives of the Biopotential group require expert knowledge. However, the overall ranking suggests that our participants may have intuitively assessed the potential privacy risks adequately.

Depending on the type of online service, we also observed that participants' perceived risk associated with the processing of biometric data by the online service provider had a negative impact on the willingness to disclose biometric traits for CAuthN purposes. Given the consistent ranking of privacy risks associated with the type of biometric traits, the perception of risk associated with an authenticating service provider holds the highest relevance, which seems to be different from traditional non-biometric authentication methods. Thus, when a CAuthN mechanism is employed by a provider associated with a high risk perception, it can lead to reduced acceptance of this technology. Our findings suggest that the use of CAuthN in Single Sign-On services offered under the name of a social media platform (e.g., Facebook [73]) may result in limited acceptance. To employ CAuthN for a wide range of online services, the adoption of a particularly trustworthy, central identity provider may be necessary. However, we note that these assumptions need

further investigation. Structural equation modeling further revealed that effects differ for the same factor for different types of online services (i.e., contextual differences) as well as for different types of biometric traits. Thus, both aspects seem to be crucial in our participants' decision to disclose biometric traits. For example, effects of response efficacy on Body-Related traits are consistently lower compared to other groups of biometric traits (cf. Fig. 5). This could be due to the fact that biometric authentication based on fingerprints or facial recognition are widely deployed in consumer products, which makes perceived efficacy of Body-Related traits in protecting accounts more apparent or understandable to lay users. We assume that once CAuthN systems based on Device Interaction and Profiling-Related traits are deployed more widely, the effect of response efficacy on willingness to disclose will decrease. Similarly, assuming that factors with negative effects on willingness to disclose, such as general privacy risk and provider-related risk remain constant, the relevance of privacy-related perceptions in the decision-making process increases.

Comparing traditional biometric authentication systems and CAuthN systems suggests that users evaluate them based on the type of authentication mechanism and the system they are securing. Traditional biometric authentication has historically been examined as a replacement for password or PIN-based entry point authentication [9, 25, 92, 104]. Researchers often concluded that participants' evaluations of appropriateness and willingness to use can be linked to the respondents' experience with corresponding biometric traits [31, 51, 93, 102–104]. Our respondents do not seem to have applied this strategy, as it is unlikely that they have consciously gained experience with authentication systems using Device Interaction or Profiling-Related traits. As a result, users prefer Body-Related traits over Device Interaction traits for traditional biometric authentication, unlike what we observed for CAuthN [25, 31, 102]. Traditional biometric authentication has predominantly been studied in the context of device authentication [9, 25, 92, 104]. Recent investigations considered biometric traits for entry point authentication in the context of various online services [103]. Researchers found that the context of the online service influenced the respondents' preferences, but the applied study design did not allow drawing conclusions about the causes. Our study helps to bridge this gap since the structural equation model demonstrates that the primary factor influencing context-dependent evaluations is the perceived risk with a service provider's processing of biometric data.

8 LIMITATIONS AND FUTURE WORK

Our study is limited to U.S. citizens on the platform Prolific. While we ensured a homogeneous sample in terms of basic demographics, the population we studied is unique, limiting the generalizability of our findings. Due to resource constraints, we had to make this trade-off, but we provided detailed demographic characteristics of our sample. From a statistical perspective, having a homogeneous population regarding usage frequency for all online service types tested would have been ideal. We focused our statements on the respective study groups to overcome this limitation. Despite variations in service usage among participants, we believe that the identified differences are practically relevant. Due to the hypothetical nature of our study, we investigated the intention to disclose biometric data to protect against a threat described only textually. However, it remains uncertain if users will act as suggested by our study when faced with real CAuthN systems that aim to protect against actual threats. Therefore, further experiments are necessary, including different biometric traits in various online service contexts, to assess users' acceptance of CAuthN in real-world scenarios.

Our survey instrument does not distinguish between the types of devices used by our participants to access online services or apps. This can lead to situations where participants primarily using mobile devices are asked to rate their willingness to share mouse dynamic data. This combination may appear illogical and could influence participants' assessments. However, we are confident that the groups of biometric traits identified through factorial analysis account for potential inconsistencies. For instance, the Device Interaction group includes biometric traits relevant to both mobile and non-mobile devices. Moreover, if participants adjusted their ratings based on the sensors available on their usual devices, our results would reflect typical device usage patterns for each online service, preserving the practical significance of our findings.

Choosing a threat model in which an attacker gains unauthorized access to an authenticated device for our survey might have been too abstract or irrelevant for our respondents, because the likelihood of unauthorized device access is potentially lower than the risk of an attack on an online account using stolen credentials. Future investigations should consider additional threat models to assess users' willingness to disclose biometric traits for CAuthN. Based on our findings, especially regarding the groups of traits identified, future work could investigate more differentiated usage scenarios of CAuthN, like local vs. remote processing of biometric traits or improvements of user experience due to reduced effort required for active re-authentications after timed-out sessions.

9 CONCLUSIONS

We surveyed 830 participants from the U.S. to examine their willingness to disclose different types of biometric traits to be used for CAuthN in the context of different apps and online service types. We identified four latent factors that reflect users' willingness to disclose different types of biometric traits, namely Body-Related, Device Interaction, Profiling-Related, and Biopotential. We provide evidence that users' willingness to disclose differs depending on the type of biometric trait and the context of the app or online service used. Whereas Device Interaction traits were generally considered to be most appropriate, participants assessed the disclosure of Body Related traits as reasonable only for contexts like Banking / Payment and Cloud Storage. We found no evidence that participants' willingness to disclose was related to the asset to be protected. Instead, willingness to disclose was mainly influenced by users' beliefs that a specific trait can help protect their account and the perceived loss of privacy related to the disclosure. Depending on the context, the risk related to the processing of biometric data by a particular service provider also had an effect on users' willingness to disclose biometric data. In conclusion, we find that acceptance of CAuthN technology depends on both the type of biometric data used and the application context. The results of our study are useful to design and develop CAuthN systems that strengthen account security while respecting internet users' privacy perceptions.

ACKNOWLEDGMENTS

We thank the members of the Data and Application Security Group for reviewing our study and especially Martha Lacek for helping us revise our survey. We would like to thank our study participants once again for their support. We thank the anonymous reviewers for their advice and insightful comments that helped us improve our work as well as for their suggestions for future research directions. This research did not receive special funding.

REFERENCES

[1] Mohammed Abuhamad, Ahmed Abusnaina, Daehun Nyang, and David Mohaisen. 2021. Sensor-Based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey. *IEEE Internet of Things Journal* 8, 1 (2021), 65–84.

[2] James Algina, H. J. Keselman, and Randall D. Penfield. 2005. An alternative to Cohen's standardized mean difference effect size: a robust parameter and confidence interval in the two independent groups case. *Psychological Methods* 10, 3 (2005), 317–328.

[3] Florian Alt and Stefan Schneegass. 2022. Beyond Passwords—Challenges and Opportunities of Future Authentication. *IEEE Security & Privacy* 20, 1 (2022), 82–86.

[4] Olga Angelopoulou, Andy Jones, Graeme Horsman, and Seyedali Pourmoafi. 2022. A Study of the Data Remaining on Second-Hand Mobile Devices in the UK. *Journal of Digital Forensics, Security and Law* 17, 2 (Oct. 2022). https://doi.org/10.58940/1558-7223.1785

[5] Adam J. Aviv, John T. Davin, Flynn Wolf, and Ravi Kuber. 2017. Towards Baselines for Shoulder Surfing on Mobile Authentication. In *Proceedings of the 33rd Annual Computer Security Applications Conference*. ACM, Orlando FL USA, 486–498. https://doi.org/10.1145/3134600.3134609

[6] Sundar Ayeswarya and Jasmine Norman. 2019. A survey on different continuous authentication systems. *International Journal of Biometrics* 11, 1 (2019), 67.

[7] Ahmed Fraz Baig and Sigurd Eskeland. 2021. Security, Privacy, and Usability in Continuous Authentication: A Survey. *Sensors (Basel, Switzerland)* 21, 17 (2021), 5967.

[8] Diane Bartz and David Shepardson. 2022. Texas Sues Google for Allegedly Capturing Biometric Data of Millions without Consent. https://www.reuters.com/legal/texas-sues-google-allegedly-capturing-biometric-data-millions-without-consent-2022-10-20/.

[9] Chandrasekhar Bhagavatula, Blase Ur, Kevin Iacovino, Su Mon Kywe, Lorrie Faith Cranor, and Marios Savvides. 2015. Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption. In *Proceedings 2015 Workshop on Usable Security*. Internet Society, San Diego, CA, 1–10. https://doi.org/10.14722/usec.2015.23003

[10] Károly Boda, Ádám Máté Földes, Gábor György Gulyás, and Sándor Imre. 2012. User Tracking on the Web via Cross-Browser Fingerprinting. In *Information Security Technology for Applications (Lecture Notes in Computer Science)*, Peeter Laud (Ed.). Springer, Berlin, Heidelberg, 31–46. https://doi.org/10.1007/978-3-642-29615-4_4

[11] Andrea Bondavalli, Ariadne Carvalho, Andrea Ceccarelli, and Enrico Schiavone. 2019. Design, implementation, and assessment of a usable multi-biometric continuous authentication system. *International Journal of Critical Computer-Based Systems* 9 (2019), 215.

[12] Darrell Carpenter, Michele Maasberg, Chelsea Hicks, and Xiaogang Chen. 2016. A Multicultural Study of Biometric Privacy Concerns in a Fire Ground Accountability Crisis Response System. *International Journal of Information Management: The Journal for Information Professionals* 36, 5 (2016), 735–747.

[13] Darrell Carpenter, Alexander McLeod, Chelsea Hicks, and Michele Maasberg. 2018. Privacy and Biometrics: An Empirical Examination of Employee Concerns. *Information Systems Frontiers* 20, 1 (2018), 91–110.

[14] Charles S. Carver and Michael F. Scheier. 2000. On the structure of behavioral self-regulation. In *Handbook of self-regulation*. Academic Press, 41–84.

[15] Angela Chau, Greg Stephens, and Rodger Jamieson. 2004. Biometrics Acceptance - Perceptions of Use of Biometrics. In *Proceedings of the Australasian Conferences on Information Systems (ACIS)*. ACIS, 1–7.

[16] Jacob Cohen. 2013. *Statistical Power Analysis for the Behavioral Sciences* (0 ed.). Routledge. https://doi.org/10.4324/9780203771587

[17] Michele Cornacchia, Filomena Papa, and Bartolomeo Sapio. 2020. User Acceptance of Voice Biometrics in Managing the Physical Access to a Secure Area of an International Airport. *Technology Analysis & Strategic Management* 32, 10 (2020), 1236–1250.

[18] Gabriel Dahia, Leone Jesus, and Maurício Pamplona Segundo. 2020. Continuous authentication using biometrics: An advanced review. *WIREs Data Mining and Knowledge Discovery* 10, 4 (2020), e1365.

[19] Naser Damer, Fabian Maul, and Christoph Busch. 2016. Multi-biometric continuous authentication: A trust model for an asynchronous system. In *Proceedings of the 19th International Conference on Information Fusion (FUSION)*. IEEE, 2192–2199.

[20] Shaveta Dargan and Munish Kumar. 2020. A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. *Expert Systems with Applications: An International Journal* 143, C (2020).

[21] Maria De Marsico, Chiara Galdi, Michele Nappi, and Daniel Riccio. 2014. FIRME: Face and Iris Recognition for Mobile Engagement. *Image and Vision Computing* 32 (2014), 1161–1172.

[22] Frank Deane, Kate Barrelle, Ron Henderson, and Doug Mahar. 1995. Perceived Acceptability of Biometric Security Systems. *Computers & Security* 14, 3 (1995), 225–231.

[23] Olive Jean Dunn. 1964. Multiple Comparisons Using Rank Sums. *Technometrics* 6, 3 (1964), 241–252.

[24] Charles D. Dziuban and Edwin C. Shirkey. 1974. When is a correlation matrix appropriate for factor analysis? Some decision rules. *Psychological Bulletin* 81 (1974), 358–361.

[25] Tim Dörflinger, Anna Voth, Juliane Krämer, and Ronald Fromm. 2010. "My smartphone is a safe!" The user's point of view regarding novel authentication methods and gradual security levels on smartphones. In *2010 International Conference on Security and Cryptography (SECRYPT)*. IEEE, 1–10.

[26] Simon Eberz, Kasper B. Rasmussen, Vincent Lenders, and Ivan Martinovic. 2017. Evaluating Behavioral Biometrics for Continuous Authentication: Challenges and Metrics. In *Proceedings of the ACM on Asia Conference on Computer and Communications Security*. Association for Computing Machinery, 386–399.

[27] Mohsen A. M. El-Bendary, Hany Kasban, Ayman Haggag, and M. A. R. El-Tokhy. 2020. Investigating of nodes and personal authentications utilizing multimodal biometrics for medical application of WBANs security. *Multimedia Tools and Applications* 79, 33 (2020), 24507–24535.

[28] European Data Protection Board. 2022. Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. (2022).

[29] European Union. 2016. General Data Protection Regulation. (2016).

[30] Cori Faklaris, Laura A. Dabbish, and Jason I. Hong. 2019. A Self-Report Measure of End-User Security Attitudes (SA-6). In *Proceedings of the 15th USENIX Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, 61–77.

[31] Steven Furnell and Konstantinos Evangelatos. 2007. Public awareness and perceptions of biometrics. *Computer Fraud & Security* 2007, 1 (Jan. 2007), 8–13. https://doi.org/10.1016/S1361-3723(07)70006-4

[32] S. M Furnell, P. S Dowland, H. M Illingworth, and P. L Reynolds. 2000. Authentication and Supervision: A Survey of User Attitudes. *Computers & Security* 19, 6 (2000), 529–539.

[33] Ramadan Gad, Nawal El-Fishawy, Ayman El-Sayed, and M. Zorkany. 2015. Multi-Biometric Systems: A State of the Art Survey and Research Directions. *International Journal of Advanced Computer Science and Applications (IJACSA)* 6, 6 (2015).

[34] Thomas Groß. 2021. Validity and Reliability of the Scale Internet Users' Information Privacy Concerns (IUIPC). *Proceedings on Privacy Enhancing Technologies* 2021, 2 (2021), 235–258.

[35] Aditi Gupta, Markus Miettinen, N. Asokan, and Marcin Nagy. 2012. Intuitive Security Policy Configuration in Mobile Devices Using Context Profiling. In *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*. IEEE, 471–480.

[36] Taban Habibu, Edith Talina Luhanga, and Anael Elikana Sam. 2019. Evaluation of Users' Knowledge and Concerns of Biometric Passport Systems. *Data* 4, 2 (2019), 58.

[37] Taban Habibu, Edith Talina Luhanga, and Anael Elikana Sam. 2022. Assessment of How Users Perceive the Usage of Biometric Technology Applications. In *Recent Advances in Biometrics*, Muhammad Sarfraz (Ed.). IntechOpen, Chapter 3.

[38] Joseph F. Hair, William C. Black, Barry J. Babin, and Rolph E. Anderson. 2019. *Multivariate Data Analysis* (eighth ed.). Cengage.

[39] Joseph F. Hair, Jeffrey R. Risher, Marko Sarstedt, and Christian M. Ringle. 2018. When to use and how to report the results of PLS-SEM. *European Business Review* 31 (Dec. 2018).

[40] Joshua Harrison, Ehsan Toreini, and Maryam Mehrnezhad. 2023. A Practical Deep Learning-Based Acoustic Side Channel Attack on Keyboards. In *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, Delft, Netherlands, 270–280. https://doi.org/10.1109/EuroSPW59978.2023.00034

[41] Jonas M. B. Haslbeck and Riet van Bork. 2022. Estimating the number of factors in exploratory factor analysis via out-of-sample prediction errors. *Psychological Methods* (2022).

[42] Taylor Hatmaker. 2021. Facebook Will Pay $650 Million to Settle Class Action Suit Centered on Illinois Privacy Law. https://techcrunch.com/2021/03/01/facebook-illinois-class-action-bipa/

[43] Myles Hollander, Douglas A. Wolfe, and Eric Chicken. 2015. *The Two-Sample Location Problem*. John Wiley and Sons, Ltd, Chapter 4, 115–150. https://doi.org/10.1002/9781119196037.ch4 arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119196037.ch4

[44] Kevin Hurler. 2022. Google Might Owe You Money for Your Face If You Live in Illinois. https://gizmodo.com/google-lawsuit-photo-privacy-illinois-1849015776.

[45] Yvonne Höller and Andreas Uhl. 2018. Do EEG-Biometric Templates Threaten User Privacy?. In *Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec '18)*. Association for Computing Machinery, New York, NY, USA, 31–42. https://doi.org/10.1145/3206004.3206006

[46] Illinois State Legislature. 2008. Biometric Information Privacy Act.

[47] Athina Ioannou, Iis Tussyadiah, and Graham Miller. 2020. That's Private! Understanding Travelers' Privacy Concerns and Online Data Disclosure. *Journal of Travel Research* (2020), 0047287520951642.

[48] ISO/IEC 2382-37:2023 2022. *Information Technology — Vocabulary — Part 37: Biometrics*. Standard. International Organization for Standardization.

[49] Jongkil Jay Jeong, Yevhen Zolotavkin, and Robin Doss. 2022. Examining the Current Status and Emerging Trends in Continuous Authentication Technologies through Citation Network Analysis. *ACM Comput. Surv.* 55, 6, Article 122 (dec 2022), 31 pages. https://doi.org/10.1145/3533705

[50] Johnston and Warkentin. 2010. Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly* 34, 3 (2010), 549.

[51] Laurie A. Jones, Annie I. Antón, and Julia B. Earp. 2007. Towards understanding user perceptions of authentication technologies. In *Proceedings of the 2007 ACM workshop on Privacy in electronic society*. ACM, Alexandria Virginia USA, 91–98. https://doi.org/10.1145/1314333.1314352

[52] Kabir O. Kasim, Scott R. Winter, Dahai Liu, Joseph R. Keebler, and Tyler B. Spence. 2021. Passengers' Perceptions on the Use of Biometrics at Airports: A Statistical Model of the Extended Theory of Planned Behavior. *Technology in Society* 67 (2021), 101806.

[53] Hassan Khan, Urs Hengartner, and Daniel Vogel. 2015. Usability and security perceptions of implicit authentication: convenient, secure, sometimes annoying. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security (SOUPS '15)*. USENIX Association, USA, 225–239.

[54] Simon Khan, Cooper Fraser, Daqing Hou, Mahesh Banavar, and Stephanie Schuckers. 2021. Authenticating Facebook Users Based on Widget Interaction Behavior. In *Proceedings of the 18th Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 1–8.

[55] Bart P. Knijnenburg, Alfred Kobsa, and Hongxia Jin. 2013. Dimensionality of Information Disclosure Behavior. *International Journal of Human-Computer Studies* 71, 12 (2013), 1144–1162.

[56] Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano. 2022. Introduction and Overview. In *Modern Socio-Technical Perspectives on Privacy*, Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano (Eds.). Springer Cham, 1–11.

[57] Aleksandra Korolova and Vinod Sharma. 2018. Cross-App Tracking via Nearby Bluetooth Low Energy Devices. In *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy (CODASPY '18)*. Association for Computing Machinery, New York, NY, USA, 43–52. https://doi.org/10.1145/3176258.3176313

[58] Andraž Krašovec, Daniel Pellarini, Dimitrios Geneiatakis, Gianmarco Baldini, and Veljko Pejović. 2020. Not Quite Yourself Today: Behaviour-Based Continuous Authentication in IoT Environments. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 4, 4 (Dec. 2020), 136:1–136:29.

[59] Rajesh Kumar, Vir V. Phoha, and Abdul Serwadda. 2016. Continuous authentication of smartphone users by fusing typing, swiping, and phone movement patterns. In *Proceedings of the 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*. IEEE, 1–8.

[60] Ruggero Donida Labati, Angelo Genovese, Enrique Muñoz, Vincenzo Piuri, Fabio Scotti, and Gianluca Sforza. 2017. Biometric Recognition in Automated Border Control: A Survey. *Comput. Surveys* 49, 2 (June 2017), 1–39. https://doi.org/10.1145/2933241

[61] Caroline Lancelot Miltgen, Aleš Popovič, and Tiago Oliveira. 2013. Determinants of End-User Acceptance of Biometrics: Integrating the "Big 3" of Technology Acceptance with Privacy Context. *Decision Support Systems* 56 (2013), 103–114.

[62] Leona Lassak, Annika Hildebrandt, Maximilian Golla, and Blase Ur. 2021. "It's Stored, Hopefully, on an Encrypted Server": Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 91–108. https://www.usenix.org/conference/usenixsecurity21/presentation/lassak

[63] Yair Levy, Michelle M. Ramim, Steven M. Furnell, and Nathan L. Clarke. 2011. Comparing Intentions to Use University-provided vs Vendor-provided Multi-biometric Authentication in Online Exams. *Campus-Wide Information Systems* 28, 2 (2011), 102–113.

[64] Tong Li, Yong Li, Mingyang Zhang, Sasu Tarkoma, and Pan Hui. 2023. You Are How You Use Apps: User Profiling Based on Spatiotemporal App Usage Behavior. *ACM Transactions on Intelligent Systems and Technology* 14, 4 (July 2023), 71:1–71:21. https://doi.org/10.1145/3597212

[65] Huigang Liang and Yajiong Xue. 2009. Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly* 33 (2009), 71–90.

[66] Bryan Cave Leighton Paisner LLP. 2022. U.S. Biometric Laws & Pending Legislation Tracker.

[67] Patrick Mair and Rand Wilcox. 2020. Robust statistical methods in R using the WRS2 package. *Behavior Research Methods* 52, 2 (April 2020), 464–488. https://doi.org/10.3758/s13428-019-01246-w

[68] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research* 15, 4 (2004), 336–355.

[69] Ereni Markos, George R. Milne, and James W. Peltier. 2017. Information Sensitivity and Willingness to Provide Continua: A Comparative Privacy Study of the United States and Brazil. *Journal of Public Policy & Marketing* 36, 1 (April 2017), 79–96.

[70] Miguel Martinho, Ana Fred, and Hugo Silva. 2018. Towards Continuous User Recognition by Exploring Physiological Multimodality: An Electrocardiogram (ECG) and Blood Volume Pulse (BVP) Approach. In *2018 International Symposium in Sensing and Instrumentation in IoT Era (ISSI)*. IEEE, 1–6.

[71] Weizhi Meng, Duncan S. Wong, Steven Furnell, and Jianying Zhou. 2015. Surveying the Development of Biometric User Authentication on Mobile Phones. *IEEE Communications Surveys & Tutorials* 17, 3 (2015), 1268–1293.

[72] George R. Milne, George Pettinico, Fatima M. Hajjat, and Ereni Markos. 2017. Information Sensitivity Typology: Mapping the Degree and Type of Risk Consumers Perceive in Personal Data Sharing. *Journal of Consumer Affairs* 51, 1 (2017), 133–161.

[73] Srivathsan G. Morkonda, Sonia Chiasson, and Paul C. van Oorschot. 2021. Empirical Analysis and Privacy Implications in OAuth-based Single Sign-On Systems. In *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*. Association for Computing Machinery, New York, NY, USA, 195–208.

[74] Cristian Morosan. 2018. Information Disclosure to Biometric E-gates: The Roles of Perceived Security, Benefits, and Emotions. *Journal of Travel Research* 57, 5 (2018), 644–657.

[75] David L. Mothersbaugh, William K. Foxx, Sharon E. Beatty, and Sijun Wang. 2012. Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information. *Journal of Service Research* 15, 1 (Feb. 2012), 76–98. https://doi.org/10.1177/1094670511424924 Publisher: SAGE Publications Inc.

[76] Rahul Murmuria, Angelos Stavrou, Daniel Barbará, and Dan Fleck. 2015. Continuous Authentication on Mobile Devices Using Power Consumption, Touch Gestures and Physical Movement of Users. In *Research in Attacks, Intrusions, and Defenses*, Herbert Bos, Fabian Monrose, and Gregory Blanc (Eds.). Springer, Cham, 405–424.

[77] NBC. 2022. Judge Approves $92 Million TikTok Settlement, With Illinois Claimants Receiving Biggest Share. https://www.nbcchicago.com/news/local/judge-approves-92-million-tiktok-settlement-with-illinois-claimants-receiving-biggest-share/2921881/

[78] Helen Nissenbaum. 2004. Privacy as Contextual Integrity. *Washington Law Review* 79, 1 (2004), 1119–157.

[79] Christian M. Olt and Amina Wagner. 2020. Having Two Conflicting Goals in Mind: The Tension Between IS Security and Privacy when Avoiding Threats. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*.

[80] Sanka Rasnayaka and Terence Sim. 2018. Who Wants Continuous Authentication on Mobile Devices?. In *Proceedings of the IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*. IEEE, 1–9.

[81] N. K. Ratha, J. H. Connell, and R. M. Bolle. 2001. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal* 40, 3 (2001), 614–634. https://doi.org/10.1147/sj.403.0614 Conference Name: IBM Systems Journal.

[82] Riseul Ryu, Soonja Yeom, Soo-Hyung Kim, and David Herbert. 2021. Continuous Multimodal Biometric Authentication Schemes: A Systematic Review. *IEEE Access* 9 (2021), 34541–34557.

[83] Maxim Schessler, Eva Gerlitz, Maximilian Häring, and Matthew Smith. 2021. Replication: Measuring User Perceptions in Smartphone Security and Privacy in Germany. In *Proceedings of the 2021 European Symposium on Usable Security* (Karlsruhe, Germany) *(EuroUSEC '21)*. Association for Computing Machinery, New York, NY, USA, 165–179. https://doi.org/10.1145/3481357.3481511

[84] Enrico Schiavone, Andrea Ceccarelli, Ariadne Carvalho, and Andrea Bondavalli. 2019. Design, implementation, and assessment of a usable multi-biometric continuous authentication system. *International Journal of Critical Computer-Based Systems* 9, 3 (Jan. 2019), 215–247.

[85] Devu Manikantan Shila and Kunal Srivastava. 2018. CASTRA: Seamless and Unobtrusive Authentication of Users to Diverse Mobile Services. *IEEE Internet of Things Journal* 5, 5 (2018), 4042–4057.

[86] Andreas Skalkos, Ioannis Stylios, Maria Karyda, and Spyros Kokolakis. 2021. Users' Privacy Attitudes towards the Use of Behavioral Biometrics Continuous Authentication (BBCA) Technologies: A Protection Motivation Theory Approach. *Journal of Cybersecurity and Privacy* 1, 4 (2021), 743–766.

[87] Ioannis Stylios, Spyros Kokolakis, Olga Thanou, and Sotirios Chatzis. 2022. Key Factors Driving the Adoption of Behavioral Biometrics and Continuous Authentication Technology: An Empirical Research. *Information & Computer Security* 30, 4 (2022), 562–582.

[88] Ioannis C. Stylios, Olga Thanou, Iosif Androulidakis, and Elena Zaitseva. 2016. A Review of Continuous Authentication Using Behavioral Biometrics. In *Proceedings of the SouthEast European Design Automation, Computer Engineering, Computer Networks and Social Media Conference*. Association for Computing Machinery, 72–79.
[89] Texas Legislature. 2009. Texas Business & Commerce Code 503.001 – Capture or Use of Biometric Identifiers Act. (2009).
[90] Maciej Tomczak and Ewa Tomczak. 2014. The need to report effect size estimates revisited. An overview of some recommended measures of effect size. *Trends in Sport Sciences* 21, 1 (2014), 19–25.
[91] Horst Treiblmaier and Sandy Chong. 2011. Trust and Perceived Risk of Personal Information as Antecedents of Online Information Disclosure: Results from Three Countries. *Journal of Global Information Management* 19 (2011), 76–94.
[92] Vasileios Tsoukas, Anargyros Gkogkidis, and Athanasios Kakarountas. 2020. A Survey on Mobile User Perceptions of Sensitive Data and Authentication Methods. In *24th Pan-Hellenic Conference on Informatics*. ACM, Athens Greece, 346–349. https://doi.org/10.1145/3437120.3437337
[93] M. Veldhuis. 2018. User preference for authentication method: A study on the influencing variables in a web application context. https://www.semanticscholar.org/paper/User-preference-for-authentication-method%3A-A-study-Veldhuis/f086540a021ef742a98103df8e5ce49e7182e91f
[94] Konstantina Vemou. 2021. Biometric Continuous Authentication | European Data Protection Supervisor. https://edps.europa.eu/press-publications/publications/techsonar/biometric-continuous-authentication
[95] Min Wang, Hussein A. Abbass, and Jiankun Hu. 2016. Continuous authentication using EEG and face images for trusted autonomous systems. In *Proceedings of the 14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 368–375.
[96] Stephan Wiefling, Paul René Jørgensen, Sigurd Thunem, and Luigi Lo Iacono. 2023. Pump Up Password Security! Evaluating and Enhancing Risk-Based Authentication on a Real-World Large-Scale Online Service. *ACM Transactions on Privacy and Security* 26, 1 (Feb. 2023), 1–36. https://doi.org/10.1145/3546069
[97] Rand Wilcox. 2012. *Introduction to robust estimation and hypothesis testing. 3rd ed.* Vol. 93. Academic Press. https://doi.org/10.2307/2669876
[98] Michael Workman, William H. Bommer, and Detmar Straub. 2008. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior* 24, 6 (2008), 2799–2816.
[99] Jain-Shing Wu, Wan-Ching Lin, Chih-Ta Lin, and Te-En Wei. 2015. Smartphone continuous authentication based on keystroke and gesture profiling. In *2015 International Carnahan Conference on Security Technology (ICCST)*. IEEE, 191–197.
[100] Lulu Yang, Chen Li, Ruibang You, Bibo Tu, and Linghui Li. 2021. TKCA: a timely keystroke-based continuous user authentication with short keystroke sequence in uncontrolled settings. *Cybersecurity* 4, 1 (2021), 13.
[101] Nan Zheng, Aaron Paloski, and Haining Wang. 2011. An Efficient User Verification System via Mouse Movements. In *Proceedings of the 18th ACM Conference on Computer and Communications Security* (Chicago, Illinois, USA) *(CCS '11)*. Association for Computing Machinery, New York, NY, USA, 139–150. https://doi.org/10.1145/2046707.2046725
[102] Verena Zimmermann and Nina Gerber. 2017. "If It Wasn't Secure, They Would Not Use It in the Movies" – Security Perceptions and User Acceptance of Authentication Technologies. In *Human Aspects of Information Security, Privacy and Trust (Lecture Notes in Computer Science)*, Theo Tryfonas (Ed.). Springer International Publishing, Cham, 265–283. https://doi.org/10.1007/978-3-319-58460-7_18
[103] Verena Zimmermann, Paul Gerber, and Alina Stöver. 2022. That Depends – Assessing User Perceptions of Authentication Schemes across Contexts of Use. http://arxiv.org/abs/2209.13958 arXiv:2209.13958 [cs].
[104] Nedaa Zirjawi, Zijad Kurtanovic, and Walid Maalej. 2015. A survey about user requirements for biometric authentication on smartphones. In *2015 IEEE 2nd Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE)*. IEEE, 1–6. https://doi.org/10.1109/ESPRE.2015.7330160
[105] Conrad Zygmont and Mario Smith. 2014. Robust factor analysis in the presence of normality violations, missing data, and outliers: Empirical questions and possible solutions. *The Quantitative Methods for Psychology* 10 (2014), 40–55.

A SURVEY

The survey presented refers to the study condition *Social Media*. Questionnaires for the other conditions differ only in the designation of the service type.

A.1 Privacy and Consent Statement

A.2 $\text{Risk}_{\text{Asset}}$ and Susceptibility

A.2.1 Contextualization with online service type.

Questions. Please name up to three actions for which you frequently use your favorite *social media* website or mobile app!

Answer options. Participants are offered three text input fields.

A.2.2 $Risk_{Asset}$. Adapted from [68].

Questions. Please rate your agreement or disagreement with the following statements.

(1) In general, it would be risky if an unauthorized person had access to my account on my favorite *social media* website or mobile app.
(2) There would be high potential for loss associated with an unauthorized person having access to my account on my favorite *social media* website or mobile app.
(3) There would be too much uncertainty if an unauthorized person had access to my account on my favorite *social media* website or mobile app.
(4) If an unauthorized person were to gain access to my account on my favorite *social media* website or mobile app, it would involve many unexpected problems.
(5) I would feel safe even if an unauthorized person had access to my account on my favorite *social media* website or mobile app.

Answer options. Strongly disagree - Disagree - Somewhat disagree - Neutral - Somewhat agree - Agree - Strongly agree.

A.2.3 Susceptibility. Adapted from [50].

Questions.

(1) My account on my favorite *social media* website or mobile app is at risk to be accessed by an unauthorized person.
(2) It is likely that my account on my favorite *social media* website or mobile app gets accessed by an unauthorized person.
(3) It is possible that my account on my favorite *social media* website or mobile app gets accessed by an unauthorized person.

Answer options. Strongly disagree - Disagree - Neutral - Agree - Strongly agree

A.3 Introduction to Continuous Authentication

The video corresponding to the service type is shown to the participants. Below the video, the voiceover is displayed with the instruction to read it only if there are technical problems with the video.

The videos for all treatment groups can be accessed at:
https://github.com/das-group/CAuthN-Study-Dataset/tree/main/explanation%20videos%20for%20survey .

Text presented. Hello and thank you for participating in our survey! It's about continuous authentication on *social media* websites or mobile apps. In the following, we will explain what this means.

Before you can use your favorite *social media* website or mobile app, you must sign in, usually with a username and password. After that, you can use the app until you log yourself out or you are automatically logged out.

If an unauthorized person gains access to the device where you are logged into the service, they can use your *social media* account on your behalf. To prevent this, the provider of the *social media* website or mobile app could continuously check whether it is actually you who is using the service while you are logged in. For this purpose, the provider can use a variety of characteristics that are related to your person. These so-called biometric traits can either be collected with sensors or are obtained through your interaction with the device, like the way you are using a keyboard, a mouse, or many other traits.

In this survey, we would like to know how you would feel about providing your biometric traits to protect your *social media* account.

A.4 Quiz

Questions.

(1) Continuous Authentication is a technology that allows operators of an online service or mobile app to determine whether an account is actually being used by a legitimate user or by an unauthorized person. *(correct)*
(2) With Continuous Authentication, biometric traits such as typing behavior on a keyboard can be analyzed during the use of an online service or mobile app to determine whether the user is a legitimate one. *(correct)*
(3) With Continuous Authentication, I have to install an app on my smartphone to get a token to login to an online service or mobile app. *(wrong)*
(4) Continuous Authentication is a technology that allows me to log in to many different online services or mobile apps with one password. *(wrong)*
(5) Continuous Authentication increases the protection of my *social media* account by continously checking if it is really me who uses the account or someone unauthorized taking over my account. *(correct)*

Answer options. Multiple choice.

A.5 Willingness to Disclose, Privacy Risk and Response Efficacy

Bevor each question group, participants are introduced to the slider instrument with a short description and the possibility to test the UI element.

A.5.1 Willingness to Disclose. Participants are presented with 16 sliders for the biometric characteristics listed in Table 2. The explanatory text noted in the table is displayed next to the slider.

Questions. How willing are you to continuously share your [name of biometric trait] data with your favorite *social media* website or mobile app to improve your account protection?

Answer options. Slider input.

A.5.2 Response Efficacy. Participants are presented with 16 sliders for the biometric characteristics listed in Table 2. The explanatory text noted in the table is displayed next to the slider.

Questions. Do you believe that continuously sharing your [name of biometric trait] data with your favorite *social media* website or mobile app would help to improve your account protection?

Answer options. Slider input.

A.5.3 Privacy Risk. Participants are presented with 16 sliders for the biometric characteristics listed in Table 2. The explanatory text noted in the table is displayed next to the slider.

Questions. How much of a risk to your privacy would it be to continuously share your [name of biometric trait] data with your favorite *social media* website or mobile app to improve your account protection?

Answer options. Slider input.

A.6 $\text{Risk}_{\text{Provider}}$ and $\text{Trust}_{\text{Provider}}$

The items for risk and trust were presented together and in random order

A.6.1 $Trust_{Provider}$. Adapted from [68].

Questions.

(1) The provider of my favorite *social media* website or mobile app would be trustworthy in handling biometric data.
(2) The provider of my favorite *social media* website or mobile app would tell the truth and fulfill promises related to biometric data provided by me.
(3) I trust that the provider of my favorite *social media* website or mobile app would keep my best interests in mind when dealing with my biometric traits.
(4) The provider of my favorite *social media* website or mobile app is in general predictable and consistent regarding the usage of my biometric traits.
(5) The provider of my favorite *social media* website or mobile app is always honest with customers when it comes to using biometric traits that I would provide.

Answer options. Strongly disagree - Disagree - Somewhat disagree - Neutral - Somewhat agree - Agree - Strongly agree.

A.6.2 $Risk_{Provider}$. Adapted from [68].

Questions. Please rate your agreement or disagreement with the following statements.

(1) In general, it would be risky to give my biometric traits to the provider of my favorite *social media* website or mobile app.
(2) There would be high potential for loss associated with giving my biometric traits to the provider of my favorite *social media* website or mobile app.
(3) There would be too much uncertainty associated with giving my biometric traits to the provider of my favorite *social media* website or mobile app.

(4) Providing the provider of my favorite *social media* website or mobile app with my biometric traits would involve many unexpected problems.
(5) I would feel safe giving my biometric traits to the provider of my favorite *social media* website or mobile app.

Answer options. Strongly disagree - Disagree - Somewhat disagree - Neutral - Somewhat agree - Agree - Strongly agree.

A.7 Security Attitudes and Information Privacy Concerns

A.7.1 Security Attitudes (SA-6). Taken from [30].

Questions. Please rate your agreement or disagreement with the following statements.

(1) I seek out opportunities to learn about security measures that are relevant to me.
(2) I am extremely motivated to take all the steps needed to keep my online data and accounts safe.
(3) Generally, I diligently follow a routine about security practices.
(4) I often am interested in articles about security threats.
(5) I always pay attention to experts' advice about the steps I need to take to keep my online data and accounts safe.
(6) I am extremely knowledgeable about all the steps needed to keep my online data and accounts safe.

Answer options. Strongly disagree - Disagree - Neutral - Agree - Strongly agree

A.7.2 Information Privacy Concerns (IUIPC-8). Taken from [34].

Questions. Please rate your agreement or disagreement with the following statements.

(1) Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
(2) Consumer control of personal information lies at the heart of consumer privacy.
(3) Companies seeking information online should disclose the way the data are collected, processed, and used.
(4) A good consumer online privacy policy should have a clear and conspicuous disclosure.
(5) It usually bothers me when online companies ask me for personal information.
(6) When online companies ask me for personal information, I sometimes think twice before providing it.
(7) It bothers me to give personal information to so many online companies.
(8) I'm concerned that online companies are collecting too much personal information about me.

Answer options. Strongly disagree - Disagree - Somewhat disagree - Neutral - Somewhat agree - Agree - Strongly agree.

B STATISTICS

Table 6: Demographics for the subsamples used in the between-group study conditions.

	Total sample	Banking & Payment	Cloud Storage	Online Shopping	Messaging	Social Media	Video Streaming	Music Streaming
Age				%				
18-24	13.7	12.2	16.5	14.2	13.2	11.5	13	15.9
25-34	34.2	30.4	33	29.1	31.1	33.1	36.6	47.7
35-44	24.3	22.6	26.1	21.6	27.4	23.1	30.9	18.7
45-54	12.8	15.7	13	13.4	10.4	16.9	10.6	8.4
55-64	10	14.8	10.4	11.9	13.2	7.7	6.5	5.6
>65	4.9	4.3	0.9	9.7	4.7	7.7	2.4	3.7
Sex				%				
Female	50.1	47	48.7	50	55.7	48.5	52.8	48.6
Male	49.9	53	51.3	50	44.3	51.5	47.2	51.4
Ethnicity				%				
Asian	5.5	4.3	3.5	6	5.7	7.7	4.9	6.5
Black	3.5	2.6	4.3	4.5	3.8	2.3	1.6	5.6
Mixed	6.1	6.1	4.3	9	6.6	3.8	8.1	4.7
Other	1.8	0.9	1.7	1.5	1.9	3.1	1.6	1.9
White	83	86.1	86.1	79.1	82.1	83.1	83.7	81.3
Employment status				%				
Full-Time	46.6	56.5	40.9	39.6	38.7	46.9	44.7	60.7
Part-Time	18.1	17.4	17.4	15.7	24.5	16.2	21.1	15
Homemaker /Retiered or Disabled	15.3	12.2	16.5	23.9	19.8	13.1	10.6	10.3
Unemployed	13.1	8.7	13.9	14.9	11.3	16.9	13.8	11.2
Other	6.9	5.2	11.3	6	5.7	6.9	9.8	2.8
Houshold Income				%				
<$10k	6.9	7.8	9.6	6	9.4	3.8	5.7	6.5
$10k–$20k	8.3	6.1	9.6	9	9.4	10	4.9	9.3
$20k–$40k	18.4	14.8	26.1	12.7	15.1	15.4	26	19.6
$40k–$60k	16.7	13	9.6	18.7	22.6	23.1	12.2	17.8
$60k–$80k	17	13	15.7	16.4	21.7	17.7	18.7	15.9
$80k–$100k	10.6	15.7	7	11.2	7.5	12.3	8.9	11.2
$100k–$150k	13.4	17.4	13	19.4	6.6	11.5	12.2	12.1
>$150k	8.7	12.2	9.6	6.7	7.5	6.2	11.4	7.5
Excluding upper bound								
Highest education level completed				%				
Doctorate degree (PhD/other)	2.8	3.5	1.7	3	0.9	5.4	3.3	0.9
Graduate degree (MA/MSc/MPhil/other)	12.7	16.5	9.6	11.9	10.4	13.8	10.6	15.9
High school diploma/A-levels	26.4	21.7	18.3	29.9	26.4	25.4	32.5	29.9
Secondary education (e.g. GED/GCSE)	2.3	1.7	0.9	2.2	2.8	3.8	3.3	0.9
Technical/community college	15.4	16.5	13.9	14.2	21.7	13.8	17.1	11.2
Undergraduate degree (BA/BSc/other)	39.6	40	54.8	38.1	35.8	36.9	31.7	41.1
Relationship status				%				
Partnership	54	63.5	51.3	59	53.8	50	54.5	44.9
Single	43.6	32.2	47	38.8	44.3	49.2	42.3	52.3

Table 7: Descriptive statistics for online service characteristics

		Banking/ Payment	Cloud Storage	Online Shopping	Messaging	Social Media	Video Streaming	Music Streaming
	n	115	115	134	106	130	123	107
$\text{Risk}_{\text{Asset}}$		32.56	29.57	31.48	29.17	28.91	25.56	24.40
$\text{Trust}_{\text{Provider}}$	*M*	21.80	20.43	18.85	17.27	14.92	16.14	17.52
$\text{Risk}_{\text{Provider}}$		22.18	22.19	24.55	25.44	27.04	28.07	26.53
$\text{Risk}_{\text{Asset}}$		2.95	5.93	4.82	5.91	5.21	7.02	7.77
$\text{Trust}_{\text{Provider}}$	*SD*	7.86	7.68	7.63	7.61	6.89	6.96	7.26
$\text{Risk}_{\text{Provider}}$		7.69	7.48	7.61	7.20	6.42	6.37	6.88
$\text{Risk}_{\text{Asset}}$		34.00	30.00	33.00	31.00	29.00	27.00	27.00
$\text{Trust}_{\text{Provider}}$	*Median*	23.00	22.00	19.00	18.00	14.00	17.00	19.00
$\text{Risk}_{\text{Provider}}$		23.00	23.00	25.50	26.00	28.00	29.00	28.00

Table 8: Pairwise comparison of online service type characteristics

		$\text{Risk}_{\text{Asset}}$	$\text{Trust}_{\text{Provider}}$	$\text{Risk}_{\text{Provider}}$
	Kruskal-Wallis	$\chi^2(6) = 161.5, p < .0001$	$\chi^2(6) = 70.4, p < .0001$	$\chi^2(6) = 68.2, p < .0001$
	Effect size	$\eta^2 = .48$	$\eta^2 = .29$	$\eta^2 = .29$
Service A	Service B	p^β	p^β	p^β
Banking / Payment	Cloud Storage	<.001***	ns	ns
Banking / Payment	Online Shopping	ns	ns	ns
Banking / Payment	Messaging	<.0001****	<.001***	.032*
Banking / Payment	Social Media	<.0001****	.000****	<.0001****
Banking / Payment	Video Streaming	<.0001****	.000****	<.0001****
Banking / Payment	Music Streaming	<.0001****	<.001***	<.001***
Cloud Storage	Online Shopping	ns	ns	ns
Cloud Storage	Messaging	ns	.046*	.029*
Cloud Storage	Social Media	ns	.000****	<.0001****
Cloud Storage	Video Streaming	<.0001****	<.001***	<.0001****
Cloud Storage	Music Streaming	<.0001****	ns	<.001***
Online Shopping	Messaging	.006**	ns	ns
Online Shopping	Social Media	<.0001****	<.001***	ns
Online Shopping	Video Streaming	<.0001****	ns	.003**
Online Shopping	Music Streaming	<.0001****	ns	ns
Messaging	Social Media	ns	ns	ns
Messaging	Video Streaming	.001**	ns	ns
Messaging	Music Streaming	<.0001****	ns	ns
Social Media	Video Streaming	.015*	ns	ns
Social Media	Music Streaming	<.001***	ns	ns
Video Streaming	Music Streaming	ns	ns	ns

Interpretation of effect size: $.01 < \eta^2 < .06$ small effect, $.06 < \eta^2 < .14$ moderate effect and $\eta^2 >= .14$ large effect [90].
β: Bonferroni adjusted (21 comparisons)

Table 9: Descriptive statistics of participants' ratings for willingness to disclose (WTD), perceived privacy risk, and response efficacy related to disclosing biometric traits in the respecting study condition.

Social Media		WTD				Privacy Risk				Response Efficacy			
		M	*SD*	*Median*	*SE*	*M*	*SD*	*Median*	*SE*	*M*	*SD*	*Median*	*SE*
$n = 130$	DI	47.91	33.58	53.88	2.95	39.73	29.46	34.25	2.58	37.27	25.80	36.88	2.26
$min = 0$	PR	33.07	26.16	29.50	2.29	67.37	21.10	65.00	1.85	44.45	24.44	49.25	2.14
$max = 100$	BR	25.51	28.49	16.12	2.50	80.58	21.38	85.75	1.88	63.39	30.25	71.12	2.65
	B	16.29	26.62	0.50	2.33	68.21	30.71	73.50	2.69	28.54	29.34	19.25	2.57
Banking / Payment		WTD				Privacy Risk				Response Efficacy			
		M	*SD*	*Median*	*SE*	*M*	*SD*	*Median*	*SE*	*M*	*SD*	*Median*	*SE*
$n = 115$	DI	57.84	33.07	65.5	3.08	31.67	26.90	24.75	2.51	40.58	30.86	37.75	2.88
$min = 0$	PR	46.33	30.34	45.0	2.83	62.03	20.65	63.00	1.93	46.95	26.44	46.75	2.47
$max = 100$	BR	51.02	34.40	51.5	3.21	65.99	28.98	76.00	2.70	75.49	25.53	83.00	2.38
	B	20.89	29.98	4.5	2.80	66.15	32.19	72.00	3.00	26.28	32.21	9.50	3.00
Cloud Storage		WTD				Privacy Risk				Response Efficacy			
		M	*SD*	*Median*	*SE*	*M*	*SD*	*Median*	*SE*	*M*	*SD*	*Median*	*SE*
$n = 115$	DI	57.68	32.00	64.75	2.98	30.60	25.55	25.00	2.38	44.70	29.35	42.50	2.74
$min = 0$	PR	47.84	28.75	50.50	2.68	60.06	21.34	60.75	1.99	50.84	27.08	53.75	2.53
$max = 100$	BR	42.93	31.62	35.75	2.95	71.13	25.85	79.75	2.41	71.81	27.14	80.00	2.53
	B	23.26	28.89	11.50	2.69	62.70	32.61	67.50	3.04	32.58	31.80	26.00	2.97
Online Shopping		WTD				Privacy Risk				Response Efficacy			
		M	*SD*	*Median*	*SE*	*M*	*SD*	*Median*	*SE*	*M*	*SD*	*Median*	*SE*
$n = 134$	DI	50.99	32.73	53.00	2.83	33.22	28.79	27.88	2.49	41.15	27.88	39.12	2.41
$min = 0$	PR	42.42	28.78	41.75	2.49	61.45	22.13	63.25	1.91	50.54	24.28	51.25	2.10
$max = 100$	BR	33.74	31.03	28.38	2.68	76.20	24.33	81.50	2.10	69.92	25.91	75.00	2.24
	B	19.61	28.91	0.00	2.50	62.41	33.84	69.00	2.92	27.90	30.18	18.25	2.61
Messaging		WTD				Privacy Risk				Response Efficacy			
		M	*SD*	*Median*	*SE*	*M*	*SD*	*Median*	*SE*	*M*	*SD*	*Median*	*SE*
$n = 106$	DI	52.65	33.65	56.12	3.27	35.59	27.57	28.38	2.68	45.44	29.20	48.62	2.84
$min = 0$	PR	40.82	27.69	42.12	2.69	66.61	20.40	66.50	1.98	50.45	26.34	55.00	2.56
$max = 100$	BR	34.13	32.38	24.38	3.15	77.59	24.04	85.62	2.34	71.69	26.79	78.88	2.60
	B	19.68	29.49	2.50	2.86	68.36	31.44	75.50	3.05	34.81	32.34	27.75	3.14
Video Streaming		WTD				Privacy Risk				Response Efficacy			
		M	*SD*	*Median*	*SE*	*M*	*SD*	*Median*	*SE*	*M*	*SD*	*Median*	*SE*
$n = 123$	DI	35.02	30.39	31.00	2.74	41.22	26.06	35.75	2.35	33.07	24.11	31.75	2.17
$min = 0$	PR	35.26	25.69	32.75	2.32	63.94	20.35	63.75	1.84	49.97	23.60	52.75	2.13
$max = 100$	BR	19.08	26.44	7.00	2.38	82.64	21.20	92.00	1.91	64.41	29.28	71.25	2.64
	B	8.96	19.78	0.00	1.78	70.74	30.33	77.00	2.73	24.01	26.79	17.50	2.42
Music Streaming		WTD				Privacy Risk				Response Efficacy			
		M	*SD*	*Median*	*SE*	*M*	*SD*	*Median*	*SE*	*M*	*SD*	*Median*	*SE*
$n = 107$	DI	44.64	31.24	48.00	3.02	35.28	26.19	26.75	2.53	38.66	26.76	37.5	2.59
$min = 0$	PR	36.64	27.29	30.50	2.64	62.26	19.72	61.25	1.91	48.24	23.92	49.5	2.31
$max = 100$	BR	22.47	24.79	13.25	2.40	80.94	20.23	86.75	1.96	67.47	27.90	76.0	2.70
	B	11.99	21.05	0.00	2.03	67.31	29.75	75.50	2.8	31.19	29.97	24.5	2.90

DI: Device Interaction, PR: Profiling-Related, BR: Body-Related, B: Biopotential

Table 10: ANOVA for WTD Social Media

$F(2.48, 190.59) = 67.92, p < .001$; $\xi = 0.5$				
comp.	$\hat{\psi}$	CI_{95}	p	$p_{crit.}$
BR vs. DI	-17.92	[-25.99, -9.85]	**<.001**	.017
BR vs. PR	-8.19	[-13.26, -3.11]	**<.001**	.025
BR vs. B	6.40	[2.23, 10.57]	**<.001**	.050
DI vs. PR	12.06	[7.17, 16.95]	**<.001**	.010
DI vs. B	27.65	[18.69, 36.62]	**<.001**	.009
PR vs. B	14.11	[8.37, 19.86]	**<.001**	.013

ξ: Explanatory effect size.
Interpretation: 0.1: small, 0.3: medium, 0.5: large [67].

DI: Device Interaction, PR: Profiling-Related,
BR: Body-Related, B: Biopotential

Table 11: ANOVA for WTD Banking / Payment

$F(2.57, 208.3) = 76.71, p < .001$; $\xi = 0.16$				
comp.	$\hat{\psi}$	CI_{95}	p	$p_{crit.}$
BR vs. DI	-5.72	[-12.50, 1.07]	.025	.025
BR vs. PR	3.84	[-2.46, 10.14]	.102	.05
BR vs. B	26.69	[16.72, 36.66]	**<.001**	.013
DI vs. B	10.49	[5.27, 15.7]	**<.001**	.017
DI vs. B	35.2	[23.77, 46.63]	**<.001**	.009
PR vs. B	22.11	[13.91, 30.32]	**<.001**	.01

See notes Table 10

Table 12: ANOVA for WTD Video Streaming

$F(2.31, 170.82) = 59.03, p < .001$; $\xi = 0.43$				
comp.	$\hat{\psi}$	CI_{95}	p	$p_{crit.}$
BR vs. DI	-13.39	[-20.37, -6.41]	**<.001**	.017
BR vs. PR	-16.66	[-22.92, -10.4]	**<.001**	0.013
BR vs. B	4.92	[1.69, 8.16]	**<.001**	.025
DI vs. PR	-1.0	[-5.83, 3.83]	.575	.05
DI vs. B	22.27	[14.15, 30.39]	**<.001**	.010
PR vs. B	24.24	[17.24, 31.24]	**<.001**	0.009

See notes Table 10

Table 13: ANOVA for WTD Music Streaming

$F(2.54, 162.65) = 59.42, p < .001$; $\xi = 0.51$				
comp.	$\hat{\psi}$	CI_{95}	p	$p_{crit.}$
BR vs. DI	-20.08	[-29.24, -10.93]	**<.001**	.013
BR vs. PR	-12.11	[-18.31, -5.91]	**<.001**	.017
BR vs. B	7.97	[3.19, 12.74]	**<.001**	.025
DI vs. PR	8.12	[2.88, 13.36]	**<.001**	.05
DI vs. B	29.25	[18.98, 39.53]	**<.001**	.009
PR vs. B	21.79	[13.65, 29.93]	**<.001**	.01

See notes Table 10

Table 14: ANOVA for WTD Online Shopping

$F(2.57, 208.3) = 76.71, p < .001$; $\xi = 0.37$				
comp.	$\hat{\psi}$	CI_{95}	p	$p_{crit.}$
BR vs. DI	-15.04	[-22.12, -7.95]	**<.001**	.017
BR vs. PR	-9.09	[-13.96, -4.21]	**<.001**	.025
BR vs. B	10.30	[5.61, 14.99]	**<.001**	.013
DI vs. PR	6.59	[1.68, 11.5]	**<.001**	.05
DI vs. B	28.26	[19.13, 37.39]	**<.001**	.01
PR vs. B	21.58	[14.98, 28.18]	**<.001**	.009

See notes Table 10

Table 15: ANOVA for WTD Cloud Storage

$F(3, 204) = 68.32, p < .001$; $\xi = 0.37$				
comp.	$\hat{\psi}$	CI_{95}	p	$p_{crit.}$
BR vs. DI	-12.36	[-19.92, -4.79]	**<.001**	.017
BR vs. PR	-5.45	[-12.15, 1.25]	**.031**	.05
BR vs. B	17.95	[10.89, 25.01]	**<.001**	.013
DI vs. PR	8.16	[1.64, 14.67]	**.001**	.025
DI vs. B	32.35	[22.39, 42.31]	**<.001**	.009
PR vs. B	23.44	[15.39, 31.49]	**<.001**	0.01

See notes Table 10

Table 16: ANOVA for WTD Messaging

$F(2.61, 164.16) = 62.54, p < .001$; $\xi = 0.41$				
comp.	$\hat{\psi}$	CI_{95}	p	$p_{crit.}$
BR vs. DI	-14.0	[-22.26, -5.74]	**<.001**	.025
BR vs. PR	-5.12	[-12.33, 2.08]	.057	.05
BR vs. B	11.55	[5.86, 17.24]	**<.001**	.013
DI vs. PR	10.84	[5.17, 16.5]	**<.001**	.017
DI vs. B	29.88	[19.89, 39.86]	**<.001**	.009
PR vs. B	19.62	[12.32, 26.91]	**<.001**	.01

See notes Table 10

Table 17: ANOVA for WTD across online service types surveyed

			Device Interaction		Profiling Related		Body Related		Biopotential	
$n = 830$			$\chi^2(6) = 41.3, p < .001$ $\eta^2 = .043$		$\chi^2(6) = 25.8, p < .001$ $\eta^2 = .024$		$\chi^2(6) = 82.9, p < .001$ $\eta^2 = .093$		$\chi^2(6) = 25.0, p < .001$ $\eta^2 = .023$	
comp.	n_1	n_2	z	p^β	z	p^β	z	p^β	z	p^β
1 vs. 2	115	115	-0.01	ns	0.55	ns	-1.12	ns	0.89	ns
1 vs. 3	115	106	-1.13	ns	-1.24	ns	-3.27	**.023***	-0.81	ns
1 vs. 4	115	107	-2.94	ns	-2.30	ns	-5.77	**<.0001******	-0.32	ns
1 vs. 5	115	134	-1.62	ns	-0.94	ns	-3.71	**.004****	-1.24	ns
1 vs. 6	115	130	-2.32	ns	-3.42	**.013***	-5.69	**<.0001******	-3.35	**.017***
1 vs. 7	115	123	-5.27	**<.0001******	-2.76	ns	-7.30	**<.0001******	-2.35	ns
2 vs. 3	115	106	-1.12	ns	-1.78	ns	-2.17	ns	-1.73	ns
2 vs. 4	115	107	-2.93	ns	-2.84	ns	-4.66	**<.0001******	-1.19	ns
2 vs. 5	115	134	-1.61	ns	-1.51	ns	-2.55	ns	-2.15	ns
2 vs. 6	115	130	-2.31	ns	-3.99	**.001****	-4.54	**<.001*****	-4.25	**<.001*****
2 vs. 7	115	123	-5.27	**<.0001******	-3.32	**.019***	-6.16	**<.0001******	-3.22	**.027***
3 vs. 4	106	107	-1.77	ns	-1.03	ns	-2.44	ns	0.46	ns
3 vs. 5	106	134	-0.41	ns	0.37	ns	-0.25	ns	-0.45	ns
3 vs. 6	106	130	-1.10	ns	-2.07	ns	-2.21	ns	-2.66	ns
3 vs. 7	106	123	-4.01	**.001****	-1.44	ns	-3.83	**.003****	-1.64	ns
4 vs. 5	107	134	1.46	ns	1.46	ns	2.33	ns	-0.89	ns
4 vs. 6	107	130	0.75	ns	-0.99	ns	0.35	ns	-2.96	ns
4 vs. 7	107	123	-2.19	ns	-0.38	ns	-1.30	ns	-1.99	ns
5 vs. 6	134	130	-0.74	ns	-2.59	ns	-2.09	ns	-2.19	ns
5 vs. 7	134	123	-3.83	**.003****	-1.91	ns	-3.80	**.003****	-1.20	ns
6 vs. 7	130	123	-3.08	**.043***	0.64	ns	-1.73	ns	0.90	ns

1: Banking and Payment; 2: Cloud Storage; 3: Messaging; 4: Music Streaming, 5: Online Shopping, 6: Social Media; 7: Video Streaming
β: Bonferroni adjusted (21 comparisons)
Effect sizes: $.01- < \eta^2 < .06$: small effect; $.06 \leq \eta^2 < .14$: moderate effect; $\eta^2 \geq .14$: large effect [16]

Table 18: PLS-SEM for Banking / Payment

Banking / Payment				HTMT matrix with AVE on main diagonal											
	α	ρ_A	ρ_c	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
1	.91	.91	.94	.78†										1.18‡		
2	.92	.92	.94	.28	.80†										1.68‡	
3	.68	.72	.80	.70	.49	.51†										1.30‡
4	.95	.95	.96	.25	.42	.32	.87†							1.22‡		
5	.91	.92	.94	.35	.43	.34	.38	.79†							1.44‡	
6	.85	.85	.90	.23	.28	.36	.68	.41	.69†							1.22‡
7	.93	.93	.95	.39	.67	.49	.43	.59	.42	.78†				2.61‡	3.33‡	2.68‡
8	.63	-.54	.01	.15	.19	.35	.22	.16	.20	.18	.15†			1.05‡	1.06‡	1.06‡
9	.78	.97	.86	.08	.08	.18	.09	.08	.13	.07	.30	.68†		1.01‡	1.01‡	1.00‡
10	.94	.95	.96	.37	.50	.51	.36	.48	.25	.81	.21	.09	.82†	2.42‡	2.40‡	2.51‡
11	.94	.94	.96	.60	.37	.50	.64	.52	.55	.59	.13	.08	.46	.85†		
12	.89	.89	.92	.28	.80	.37	.42	.69	.41	.81	.17	.08	.60	.59	.75†	
13	.87	.87	.91	.43	.44	.68	.47	.49	.69	.69	.17	.12	.59	.77	.67	.72†

MV Prediction			
A	.49^{q}	25.70^{p}	29.70^{l}
B	.49^{q}	26.82^{p}	31.90^{l}
C	.37^{q}	28.58^{p}	32.92^{l}
D	.38^{q}	27.71^{p}	32.38^{l}
E	.50^{q}	29.28^{p}	34.02^{l}
F	.44^{q}	30.52^{p}	36.83^{l}
G	.51^{q}	27.66^{p}	31.58^{l}
H	.43^{q}	28.74^{p}	35.76^{l}
I	.38^{q}	28.12^{p}	31.50^{l}
J	.36^{q}	28.63^{p}	33.89^{l}
K	.41^{q}	28.39^{p}	30.62^{l}
L	.36^{q}	28.62^{p}	34.79^{l}

Constructs	**Factor Loadings** λ_1	λ_2	λ_3	λ_4	λ_5
1: Privacy Risk$_{\text{Device Interaction}}$	.84	.93	.87	.89	
2: Privacy Risk$_{\text{Body-Related}}$	.92	.87	.92	.87	
3: Privacy Risk$_{\text{Profiling-Related}}$	.77	.67	.83	.55	
4: Response Efficacy$_{\text{Device Interaction}}$	.93	.95	.90	.95	
5: Response Efficacy$_{\text{Body-Related}}$	.93	.86	.92	.84	
6: Response Efficacy$_{\text{Profiling-Related}}$	.87	.82	.85	.78	
7: Risk$_{\text{Provider}}$	.91	.87	.93	.80	.89
8: Risk$_{\text{Asset}}$	.46	.35	-.58	.18	-.20
9: Susceptibility$_{\text{Asset}}$	.78	.77	.91		
10: Trust$_{\text{Provider}}$	.91	.93	.93	.84	.91
11: WTD$_{\text{Device Interaction}}$	.94	.96	.88	.90	
12: WTD$_{\text{Body-Related}}$	.90	.84	.90	.82	
13: WTD$_{\text{Profiling-Related}}$	.92	.79	.86	.82	

ρ_α: Cronbach's alpha
ρ_A: Reliability coefficient
ρ_c: Composite reliability
$\dagger$: AVE
$\ddagger$: VIF
^{q}: Q^2_{predict}
^{p}: RMSE$_{\text{PLSpredict}}$
^{l}: RMSE$_{\text{LM}}$

LV Prediction

Q^2_{predict}	RMSE
.51	.71
.63	.62
.53	.70

A: WTD$_{\text{Keystroke Dynamics}}$
B: WTD$_{\text{Mouse Dynamics}}$
C: WTD$_{\text{Device Movement}}$
D: WTD$_{\text{Touch Dynamics}}$
E: WTD$_{\text{Face Recognition}}$
F: WTD$_{\text{Fingerprint Recognition}}$
G: WTD$_{\text{Iris Recognition}}$
H: WTD$_{\text{Voice Recognition}}$
I: WTD$_{\text{Connectivity Data}}$
J: WTD$_{\text{Device Statistics}}$
K: WTD$_{\text{Location Data}}$
L: WTD$_{\text{Usage Profiling}}$

Table 19: PLS-SEM for Cloud Storage

Cloud Storage				HTMT matrix with AVE on main diagonal												
	α	ρ_A	ρ_c	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
1	.90	.90	.93	.77†										1.13‡		
2	.88	.88	.91	.19	.73†										1.37‡	
3	.72	.74	.83	.43	.34	.54†										1.16‡
4	.93	.93	.95	.16	.25	.20	.83†							1.16‡		
5	.93	.93	.95	.25	.32	.23	.46	.83†							1.26‡	
6	.85	.86	.90	.16	.22	.30	.72	.53	.69†							1.25‡
7	.92	.93	.94	.37	.52	.30	.36	.48	.47	.76†				2.80‡	3.14‡	2.85‡
8	.90	.94	.93	.10	.21	.12	.13	.08	.09	.14	.72†			1.03‡	1.04‡	1.02‡
9	.83	.98	.90	.09	.09	.25	.07	.19	.24	.31	.08	.74†		1.10‡	1.10‡	1.12‡
10	.95	.96	.96	.23	.27	.15	.23	.33	.28	.79	.11	.21	.84†	2.28‡	2.33‡	2.38‡
11	.94	.94	.96	.63	.31	.30	.57	.55	.52	.61	.18	.12	.50	.84†		
12	.87	.88	.91	.25	.72	.14	.47	.57	.43	.70	.29	.22	.50	.63	.72†	
13	.84	.85	.89	.24	.34	.67	.55	.46	.75	.59	.12	.15	.43	.71	.56	.68†

MV Prediction			
A	.52^{q}	24.64^{p}	28.98^{l}
B	.53^{q}	23.68^{p}	24.44^{l}
C	.48^{q}	25.21^{p}	26.94^{l}
D	.44^{q}	26.36^{p}	29.98^{l}
E	.44^{q}	29.15^{p}	36.03^{l}
F	.31^{q}	31.22^{p}	34.62^{l}
G	.45^{q}	28.06^{p}	34.43^{l}
H	.30^{q}	29.89^{p}	35.29^{l}
I	.47^{q}	26.88^{p}	32.40^{l}
J	.33^{q}	28.04^{p}	31.58^{l}
K	.36^{q}	27.85^{p}	34.49^{l}
L	.42^{q}	26.16^{p}	28.60^{l}

Constructs	**Factor Loadings** λ_1	λ_2	λ_3	λ_4	λ_5
1: Privacy Risk$_{\text{Device Interaction}}$	.86	.91	.82	.90	
2: Privacy Risk$_{\text{Body-Related}}$	.86	.82	.83	.90	
3: Privacy Risk$_{\text{Profiling-Related}}$	.72	.75	.62	.85	
4: Response Efficacy$_{\text{Device Interaction}}$	.88	.95	.89	.92	
5: Response Efficacy$_{\text{Body-Related}}$	.93	.92	.93	.86	
6: Response Efficacy$_{\text{Profiling-Related}}$	.88	.75	.84	.84	
7: Risk$_{\text{Provider}}$	.93	.80	.91	.85	.88
8: Risk$_{\text{Asset}}$	.88	.86	.82	.81	.85
9: Susceptibility$_{\text{Asset}}$	.93	.84	.80		
10: Trust$_{\text{Provider}}$	.95	.95	.92	.85	.92
11: WTD$_{\text{Device Interaction}}$	.92	.95	.87	.92	
12: WTD$_{\text{Body-Related}}$	.90	.76	.92	.80	
13: WTD$_{\text{Profiling-Related}}$	.85	.82	.81	.83	

ρ_α: Cronbach's alpha
ρ_A: Reliability coefficient
ρ_c: Composite reliability
$\dagger$: AVE
$\ddagger$: VIF
^{q}: Q^2_{predict}
^{p}: RMSE$_{\text{PLSpredict}}$
^{l}: RMSE$_{\text{LM}}$

LV Prediction

Q^2_{predict}	RMSE
.59	.65
.53	.70
.58	.66

A: WTD$_{\text{Keystroke Dynamics}}$
B: WTD$_{\text{Mouse Dynamics}}$
C: WTD$_{\text{Device Movement}}$
D: WTD$_{\text{Touch Dynamics}}$
E: WTD$_{\text{Face Recognition}}$
F: WTD$_{\text{Fingerprint Recognition}}$
G: WTD$_{\text{Iris Recognition}}$
H: WTD$_{\text{Voice Recognition}}$
I: WTD$_{\text{Connectivity Data}}$
J: WTD$_{\text{Device Statistics}}$
K: WTD$_{\text{Location Data}}$
L: WTD$_{\text{Usage Profiling}}$

Table 20: PLS-SEM for Online Shopping

Online Shopping				HTMT matrix with AVE on main diagonal												**MV Prediction**			
	α	ρ_A	ρ_c	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**				
1	.95	.95	.96	.87†										1.18‡						
2	.92	.92	.94	.38	.80†										1.64‡		**A**	.58^{q}	22.91^{p}	28.04^{l}
3	.79	.80	.87	.70	.81	.62†										1.45‡	**B**	.53^{q}	24.55^{p}	29.35^{l}
4	.93	.93	.95	.09	.32	.21	.82†							1.11‡			**C**	.47^{q}	26.07^{p}	30.50^{l}
5	.90	.90	.93	.54	.32	.40	.28	.76†							1.17‡		**D**	.47^{q}	25.54^{p}	30.88^{l}
6	.79	.80	.86	.47	.43	.54	.63	.72	.61†							1.39‡	**E**	.47^{q}	25.78^{p}	31.31^{l}
7	.94	.94	.95	.40	.65	.57	.31	.36	.53	.80†				2.69‡	3.31‡	2.84‡	**F**	.36^{q}	32.23^{p}	35.25^{l}
8	.89	.91	.92	.12	.09	.14	.05	.05	.13	.12	.69†			1.04‡	1.04‡	1.03‡	**G**	.40^{q}	26.56^{p}	33.76^{l}
9	.71	.95	.82	.08	.09	.08	.12	.17	.14	.11	.13	.62†		1.03‡	1.04‡	1.03‡	**H**	.39^{q}	26.37^{p}	32.77^{l}
10	.95	.96	.96	.29	.44	.50	.22	.22	.35	.80	.05	.04	.83†	2.37‡	2.40‡	2.43‡	**I**	.40^{q}	27.87^{p}	31.78^{l}
11	.94	.95	.96	.62	.41	.51	.59	.49	.69	.59	.07	.16	.46	.85†			**J**	.48^{q}	25.10^{p}	28.97^{l}
12	.89	.89	.93	.34	.76	.55	.30	.51	.50	.75	.11	.14	.54	.57	.75†		**K**	.26^{q}	31.58^{p}	35.45^{l}
13	.85	.87	.90	.49	.65	.72	.40	.54	.81	.76	.10	.13	.60	.80	.82	.70†	**L**	.44^{q}	24.04^{p}	26.91^{l}

	Factor Loadings				
Constructs	λ_1	λ_2	λ_3	λ_4	λ_5
1: Privacy Risk$_{\text{Device Interaction}}$	.93	.93	.92	.96	
2: Privacy Risk$_{\text{Body-Related}}$	.92	.86	.93	.87	
3: Privacy Risk$_{\text{Profiling-Related}}$	.79	.82	.71	.82	
4: Response Efficacy$_{\text{Device Interaction}}$	.92	.93	.87	.89	
5: Response Efficacy$_{\text{Body-Related}}$	.89	.90	.88	.82	
6: Response Efficacy$_{\text{Profiling-Related}}$	.81	.76	.75	.82	
7: Risk$_{\text{Provider}}$	.93	.84	.94	.85	.90
8: Risk$_{\text{Asset}}$	.91	.83	.90	.77	.73
9: Susceptibility$_{\text{Asset}}$	.93	.63	.76		
10: Trust$_{\text{Provider}}$	.94	.94	.94	.81	.91
11: WTD$_{\text{Device Interaction}}$	.95	.92	.90	.93	
12: WTD$_{\text{Body-Related}}$	.90	.83	.89	.85	
13: WTD$_{\text{Profiling-Related}}$	.88	.91	.67	.86	

ρ_α: Cronbach's alpha
ρ_A: Reliability coefficient
ρ_c: Composite reliability
$\dagger$: AVE
$\ddagger$: VIF
^{q}: Q^2_{predict}
^{p}: RMSE$_{\text{PLSpredict}}$
^{l}: RMSE$_{\text{LM}}$

LV Prediction

Q^2_{predict}	RMSE
.60	.64
.54	.69
.57	.66

A: WTD$_{\text{Keystroke Dynamics}}$
B: WTD$_{\text{Mouse Dynamics}}$
C: WTD$_{\text{Device Movement}}$
D: WTD$_{\text{Touch Dynamics}}$
E: WTD$_{\text{Face Recognition}}$
F: WTD$_{\text{Fingerprint Recognition}}$
G: WTD$_{\text{Iris Recognition}}$
H: WTD$_{\text{Voice Recognition}}$
I: WTD$_{\text{Connectivity Data}}$
J: WTD$_{\text{Device Statistics}}$
K: WTD$_{\text{Location Data}}$
L: WTD$_{\text{Usage Profiling}}$

Table 21: PLS-SEM for Messaging

Messaging				HTMT matrix with AVE on main diagonal												**MV Prediction**			
	α	ρ_A	ρ_c	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**				
1	.92	.93	.94	.80†										1.32‡						
2	.88	.89	.92	.37	.74†										1.52‡		**A**	.49q	25.99p	34.16l
3	.73	.80	.82	.51	.61	.54†										1.26‡	**B**	.50q	26.34p	35.05l
4	.93	.94	.95	.28	.27	.42	.83†							1.33‡			**C**	.47q	26.80p	33.89l
5	.91	.92	.94	.51	.25	.13	.49	.79†							1.19‡		**D**	.47q	26.20p	33.76l
6	.83	.83	.89	.25	.14	.36	.70	.57	.67†							1.21‡	**E**	.43q	28.13p	33.45l
7	.93	.94	.95	.42	.65	.48	.46	.39	.32	.78†				2.63‡	2.97‡	2.64‡	**F**	.42q	29.54p	33.68l
8	.85	.88	.90	.17	.09	.11	.07	.12	.14	.14	.65†			1.17‡	1.14‡	1.14‡	**G**	.37q	28.30p	31.65l
9	.85	.91	.91	.35	.18	.17	.06	.17	.11	.25	.10	.77†		1.21‡	1.09‡	1.14‡	**H**	.33q	28.16p	30.05l
10	.94	.95	.96	.36	.51	.37	.43	.40	.33	.79	.29	.31	.81†	2.85‡	2.79‡	2.78‡	**I**	.36q	27.91p	32.99l
11	.94	.94	.96	.47	.31	.43	.77	.47	.52	.49	.09	.20	.51	.86†			**J**	.43q	26.82p	30.83l
12	.91	.91	.94	.26	.69	.27	.42	.46	.24	.67	.18	.26	.62	.63	.79†		**K**	.28q	28.21p	28.95l
13	.84	.84	.89	.36	.46	.54	.70	.43	.69	.65	.23	.21	.70	.87	.75	.67†	**L**	.38q	25.22p	29.47l

	Factor Loadings				
Constructs	λ_1	λ_2	λ_3	λ_4	λ_5
1: Privacy Risk$_{\text{Device Interaction}}$	.89	.94	.86	.89	
2: Privacy Risk$_{\text{Body-Related}}$	.88	.86	.85	.85	
3: Privacy Risk$_{\text{Profiling-Related}}$	.82	.63	.83	.62	
4: Response Efficacy$_{\text{Device Interaction}}$	.92	.93	.85	.94	
5: Response Efficacy$_{\text{Body-Related}}$	.93	.93	.89	.81	
6: Response Efficacy$_{\text{Profiling-Related}}$	.83	.80	.79	.84	
7: Risk$_{\text{Provider}}$	.93	.87	.92	.83	.87
8: Risk$_{\text{Asset}}$	.90	.84	.86	.86	.51
9: Susceptibility$_{\text{Asset}}$	.91	.81	.90		
10: Trust$_{\text{Provider}}$	.92	.94	.93	.80	.91
11: WTD$_{\text{Device Interaction}}$	.92	.94	.90	.95	
12: WTD$_{\text{Body-Related}}$	.92	.83	.92	.89	
13: WTD$_{\text{Profiling-Related}}$	.85	.86	.73	.84	

ρ_α: Cronbach's alpha
ρ_A: Reliability coefficient
ρ_c: Composite reliability
†: AVE
‡: VIF
q: Q^2_{predict}
p: RMSE$_{\text{PLSpredict}}$
l: RMSE$_{\text{LM}}$

LV Prediction

Q^2_{predict}	RMSE
.56	.67
.50	.72
.54	.69

A: WTD$_{\text{Keystroke Dynamics}}$
B: WTD$_{\text{Mouse Dynamics}}$
C: WTD$_{\text{Device Movement}}$
D: WTD$_{\text{Touch Dynamics}}$
E: WTD$_{\text{Face Recognition}}$
F: WTD$_{\text{Fingerprint Recognition}}$
G: WTD$_{\text{Iris Recognition}}$
H: WTD$_{\text{Voice Recognition}}$
I: WTD$_{\text{Connectivity Data}}$
J: WTD$_{\text{Device Statistics}}$
K: WTD$_{\text{Location Data}}$
L: WTD$_{\text{Usage Profiling}}$

Table 22: PLS-SEM for Social Media

Social Media				HTMT matrix with AVE on main diagonal											
	α	ρ_A	ρ_c	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
1	.94	.94	.95	.84†										1.26‡		
2	.89	.89	.92	.36	.75†										1.85‡	
3	.82	.82	.88	.63	.55	.65†										1.36‡
4	.94	.94	.96	.32	.25	.33	.84†							1.24‡		
5	.92	.93	.94	.66	.34	.32	.42	.81†							1.27‡	
6	.80	.81	.87	.50	.20	.37	.65	.78	.63†							1.18‡
7	.92	.93	.94	.38	.71	.46	.29	.46	.39	.76†				2.70‡	3.27‡	2.73‡
8	.87	-.34	.67	.10	.16	.16	.16	.06	.17	.17	.34†			1.11‡	1.12‡	1.07‡
9	.79	.85	.87	.18	.19	.29	.31	.08	.09	.08	.13	.70†		1.11‡	1.07‡	1.11‡
10	.93	.95	.95	.32	.59	.40	.29	.40	.33	.83	.08	.08	.79†	2.51‡	2.51‡	2.50‡
11	.96	.96	.97	.63	.40	.35	.55	.58	.45	.47	.08	.25	.33	.89†		
12	.91	.91	.94	.33	.82	.28	.39	.47	.30	.72	.11	.14	.55	.62	.79†	
13	.85	.86	.90	.53	.48	.54	.47	.50	.63	.57	.10	.19	.45	.75	.71	.69†

MV Prediction			
A	.40^{q}	28.17^{p}	32.33^{l}
B	.37^{q}	28.84^{p}	33.71^{l}
C	.41^{q}	27.12^{p}	33.38^{l}
D	.38^{q}	27.79^{p}	32.93^{l}
E	.44^{q}	23.26^{p}	29.35^{l}
F	.39^{q}	27.23^{p}	32.28^{l}
G	.48^{q}	22.75^{p}	26.84^{l}
H	.40^{q}	24.86^{p}	27.59^{l}
I	.28^{q}	27.51^{p}	35.62^{l}
J	.31^{q}	27.14^{p}	35.17^{l}
K	.19^{q}	28.32^{p}	34.85^{l}
L	.16^{q}	28.06^{p}	35.63^{l}

	Factor Loadings				
Constructs	λ_1	λ_2	λ_3	λ_4	λ_5
1: Privacy Risk$_{\text{Device Interaction}}$	.90	.94	.89	.93	
2: Privacy Risk$_{\text{Body-Related}}$	.87	.83	.92	.83	
3: Privacy Risk$_{\text{Profiling-Related}}$	.84	.78	.77	.81	
4: Response Efficacy$_{\text{Device Interaction}}$	.96	.93	.85	.93	
5: Response Efficacy$_{\text{Body-Related}}$	.93	.90	.91	.87	
6: Response Efficacy$_{\text{Profiling-Related}}$	.85	.72	.82	.78	
7: Risk$_{\text{Provider}}$	.90	.90	.90	.81	.87
8: Risk$_{\text{Asset}}$	.65	.02	.57	.54	.81
9: Susceptibility$_{\text{Asset}}$	.82	.90	.79		
10: Trust$_{\text{Provider}}$	.94	.94	.92	.75	.88
11: WTD$_{\text{Device Interaction}}$	.94	.96	.92	.96	
12: WTD$_{\text{Body-Related}}$	.93	.85	.93	.84	
13: WTD$_{\text{Profiling-Related}}$	.89	.87	.79	.77	

ρ_α: Cronbach's alpha
ρ_A: Reliability coefficient
ρ_c: Composite reliability
†: AVE
‡: VIF
^{q}: Q^2_{predict}
^{p}: RMSE$_{\text{PLSpredict}}$
^{l}: RMSE$_{\text{LM}}$

LV Prediction

Q^2_{predict}	RMSE
.44	.76
.55	.69
.34	.82

A: WTD$_{\text{Keystroke Dynamics}}$
B: WTD$_{\text{Mouse Dynamics}}$
C: WTD$_{\text{Device Movement}}$
D: WTD$_{\text{Touch Dynamics}}$
E: WTD$_{\text{Face Recognition}}$
F: WTD$_{\text{Fingerprint Recognition}}$
G: WTD$_{\text{Iris Recognition}}$
H: WTD$_{\text{Voice Recognition}}$
I: WTD$_{\text{Connectivity Data}}$
J: WTD$_{\text{Device Statistics}}$
K: WTD$_{\text{Location Data}}$
L: WTD$_{\text{Usage Profiling}}$

Table 23: PLS-SEM for Video Streaming

Video Streaming				HTMT matrix with AVE on main diagonal												
	α	ρ_A	ρ_c	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
1	.89	.90	.93	.76†										1.15‡		
2	.87	.89	.91	.33	.73†										1.55‡	
3	.72	.73	.83	.57	.37	.54†										1.25‡
4	.88	.90	.92	.22	.09	.29	.74†							1.10‡		
5	.91	.92	.94	.49	.10	.27	.37	.79†							1.12‡	
6	.78	.78	.86	.18	.12	.30	.53	.66	.60†							1.06‡
7	.90	.91	.93	.32	.60	.28	.22	.31	.10	.71†				1.96‡	2.20‡	1.94‡
8	.89	.98	.91	.10	.15	.42	.13	.09	.10	.13	.67†			1.04‡	1.03‡	1.14‡
9	.80	.86	.87	.17	.22	.25	.05	.13	.13	.15	.19	.70†		1.06‡	1.08‡	1.09‡
10	.93	.95	.95	.29	.56	.24	.24	.25	.12	.73	.10	.18	.79†	1.97‡	2.04‡	1.95‡
11	.93	.94	.95	.54	.27	.40	.62	.26	.23	.35	.15	.24	.45	.83†		
12	.88	.88	.92	.35	.69	.23	.22	.35	.10	.71	.15	.32	.63	.55	.73†	
13	.80	.82	.87	.43	.34	.68	.43	.39	.68	.36	.07	.25	.41	.69	.53	.63†

MV Prediction			
A	.38^{q}	26.35^{p}	31.57^{l}
B	.43^{q}	26.43^{p}	30.62^{l}
C	.34^{q}	25.80^{p}	28.23^{l}
D	.51^{q}	23.48^{p}	28.46^{l}
E	.38^{q}	23.15^{p}	27.80^{l}
F	.33^{q}	28.83^{p}	31.44^{l}
G	.28^{q}	25.75^{p}	32.31^{l}
H	.39^{q}	23.20^{p}	26.30^{l}
I	.28^{q}	28.49^{p}	33.98^{l}
J	.36^{q}	26.12^{p}	29.57^{l}
K	.20^{q}	29.40^{p}	30.64^{l}
L	.38^{q}	24.56^{p}	28.59^{l}

	Factor Loadings				
	λ_1	λ_2	λ_3	λ_4	λ_5
1: Privacy Risk$_{\text{Device Interaction}}$	.87	.92	.83	.86	
2: Privacy Risk$_{\text{Body-Related}}$	.87	.86	.93	.74	
3: Privacy Risk$_{\text{Profiling-Related}}$	.79	.76	.66	.74	
4: Response Efficacy$_{\text{Device Interaction}}$	.88	.90	.76	.89	
5: Response Efficacy$_{\text{Body-Related}}$	.92	.92	.88	.83	
6: Response Efficacy$_{\text{Profiling-Related}}$	.82	.78	.75	.75	
7: Risk$_{\text{Provider}}$	.88	.88	.83	.80	.82
8: Risk$_{\text{Asset}}$	.85	.93	.83	.93	.45
9: Susceptibility$_{\text{Asset}}$	.81	.87	.81		
10: Trust$_{\text{Provider}}$	.93	.89	.91	.83	.88
11: WTD$_{\text{Device Interaction}}$	.93	.95	.82	.95	
12: WTD$_{\text{Body-Related}}$	.93	.83	.87	.78	
13: WTD$_{\text{Profiling-Related}}$	.85	.85	.67	.80	

ρ_α: Cronbach's alpha
ρ_A: Reliability coefficient
ρ_c: Composite reliability
†: AVE
‡: VIF
^{q}: Q^2_{predict}
^{p}: RMSE$_{\text{PLSpredict}}$
^{l}: RMSE$_{\text{LM}}$

LV Prediction

Q^2_{predict}	RMSE
.50	.71
.49	.74
.49	.72

A: WTD$_{\text{Keystroke Dynamics}}$
B: WTD$_{\text{Mouse Dynamics}}$
C: WTD$_{\text{Device Movement}}$
D: WTD$_{\text{Touch Dynamics}}$
E: WTD$_{\text{Face Recognition}}$
F: WTD$_{\text{Fingerprint Recognition}}$
G: WTD$_{\text{Iris Recognition}}$
H: WTD$_{\text{Voice Recognition}}$
I: WTD$_{\text{Connectivity Data}}$
J: WTD$_{\text{Device Statistics}}$
K: WTD$_{\text{Location Data}}$
L: WTD$_{\text{Usage Profiling}}$

Table 24: PLS-SEM for Music Streaming

Music Streaming				HTMT matrix with AVE on main diagonal												
	α	ρ_A	ρ_c	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
1	.91	.92	.94	.79†										1.15‡		
2	.85	.85	.90	.20	.69†										1.55‡	
3	.73	.73	.83	.59	.60	.55†										1.25‡
4	.92	.94	.94	.12	.13	.27	.80†							1.10‡		
5	.93	.97	.95	.45	.14	.25	.40	.83†							1.12‡	
6	.79	.79	.86	.42	.26	.40	.66	.62	.61†							1.06‡
7	.92	.93	.94	.29	.71	.57	.27	.32	.47	.75†				1.96‡	2.20‡	1.94‡
8	.92	.98	.93	.22	.12	.17	.07	.09	.16	.21	.71†			1.04‡	1.03‡	1.14‡
9	.84	.42	.84	.11	.10	.16	.16	.05	.26	.10	.21	.65†		1.06‡	1.08‡	1.09‡
10	.95	.95	.96	.33	.60	.39	.33	.39	.54	.83	.06	.07	.83†	1.97‡	2.04‡	1.95‡
11	.93	.93	.95	.63	.19	.42	.50	.50	.56	.46	.11	.08	.40	.83†		
12	.85	.85	.90	.27	.73	.39	.15	.30	.28	.63	.10	.14	.61	.46	.69†	
13	.85	.86	.90	.50	.39	.74	.37	.42	.75	.60	.08	.13	.55	.69	.57	.70†

MV Prediction			
A	.37^{q}	28.77^{p}	37.61^{l}
B	.41^{q}	27.77^{p}	34.85^{l}
C	.30^{q}	27.08^{p}	38.28^{l}
D	.41^{q}	25.93^{p}	35.92^{l}
E	.24^{q}	25.75^{p}	35.41^{l}
F	.36^{q}	27.36^{p}	34.87^{l}
G	.27^{q}	24.50^{p}	33.27^{l}
H	.19^{q}	25.94^{p}	32.04^{l}
I	.38^{q}	26.19^{p}	37.11^{l}
J	.39^{q}	26.62^{p}	33.48^{l}
K	.29^{q}	25.03^{p}	31.56^{l}
L	.40^{q}	26.85^{p}	36.42^{l}

	Factor Loadings				
	λ_1	λ_2	λ_3	λ_4	λ_5
1: Privacy Risk$_{\text{Device Interaction}}$	.89	.94	.79	.91	
2: Privacy Risk$_{\text{Body-Related}}$	.84	.82	.85	.82	
3: Privacy Risk$_{\text{Profiling-Related}}$	.79	.77	.64	.77	
4: Response Efficacy$_{\text{Device Interaction}}$	.93	.90	.86	.89	
5: Response Efficacy$_{\text{Body-Related}}$	.93	.96	.90	.84	
6: Response Efficacy$_{\text{Profiling-Related}}$	.81	.78	.74	.78	
7: Risk$_{\text{Provider}}$	.90	.84	.90	.80	.90
8: Risk$_{\text{Asset}}$	.85	.82	.91	.75	.87
9: Susceptibility$_{\text{Asset}}$	.95	.86	.54		
10: Trust$_{\text{Provider}}$	.95	.92	.92	.85	.92
11: WTD$_{\text{Device Interaction}}$	.92	.88	.89	.94	
12: WTD$_{\text{Body-Related}}$	.86	.80	.90	.74	
13: WTD$_{\text{Profiling-Related}}$	.88	.80	.81	.85	

ρ_α: Cronbach's alpha
ρ_A: Reliability coefficient
ρ_c: Composite reliability
$\dagger$: AVE
$\ddagger$: VIF
^{q}: Q^2_{predict}
^{p}: RMSE$_{\text{PLSpredict}}$
^{l}: RMSE$_{\text{LM}}$

LV Prediction

Q^2_{predict}	RMSE
.45	.76
.39	.81
.53	.70

A: WTD$_{\text{Keystroke Dynamics}}$
B: WTD$_{\text{Mouse Dynamics}}$
C: WTD$_{\text{Device Movement}}$
D: WTD$_{\text{Touch Dynamics}}$
E: WTD$_{\text{Face Recognition}}$
F: WTD$_{\text{Fingerprint Recognition}}$
G: WTD$_{\text{Iris Recognition}}$
H: WTD$_{\text{Voice Recognition}}$
I: WTD$_{\text{Connectivity Data}}$
J: WTD$_{\text{Device Statistics}}$
K: WTD$_{\text{Location Data}}$
L: WTD$_{\text{Usage Profiling}}$