Article

Users' Privacy Attitudes towards the Use of Behavioral Biometrics Continuous Authentication (BBCA) Technologies: A Protection Motivation Theory Approach

Andreas Skalkos *, Ioannis Stylios, Maria Karyda and Spyros Kokolakis

Department of Information and Communication Systems Engineering, University of the Aegean, 83200 Samos, Greece; istylios@aegean.gr (I.S.); mka@aegean.gr (M.K.); sak@aegean.gr (S.K.)
* Correspondence: ask@aegean.gr

Abstract: Smartphone user authentication based on passwords, PINs, and touch patterns raises several security concerns. Behavioral Biometrics Continuous Authentication (BBCA) technologies provide a promising solution which can increase smartphone security and mitigate users' concerns. Until now, research in BBCA technologies has mainly focused on developing novel behavioral biometrics continuous authentication systems and their technical characteristics, overlooking users' attitudes towards BBCA. To address this gap, we conducted a study grounded on a model that integrates users' privacy concerns, trust in technology, and innovativeness with Protection Motivation Theory. A cross-sectional survey among 778 smartphone users was conducted via Amazon Mechanical Turk (MTurk) to explore the factors which can predict users' intention to use BBCA technologies. Our findings demonstrate that privacy concerns towards intention to use BBCA technology have a significant impact on all components of PMT. Further to this, another important construct we identified that affects the usage intention of BBCA technology is innovativeness. Our findings posit the view that reliability and trustworthiness of security technologies, such as BBCA are important for users. Together, these results highlighted the importance of addressing users' perceptions regarding BBCA technology.

Keywords: behavioral biometrics; continuous authentication; privacy concerns; protection motivation theory

1. Introduction

Smartphones have become an indispensable part of our lives as they are used for various aspects of people's daily activities. Besides communicating with others, we also use smartphones as cameras, notebooks, digital wallets, etc. Additionally, we exchange data and conduct payments using Near Field Communication (NFC) and control other devices through Bluetooth and WiFi. As a result, we keep a lot of personal data stored in our smartphones (e.g., videos, photos, credit card numbers, PINs, bank accounts, etc.). Currently, due to the COVID pandemic crisis, we also use smartphones for health issues, such as contact tracing, which entails storing data about our physical contacts [1]. The usefulness of smartphones has boosted them to the top of the most used devices on the web today, keeping a 55% of the global market share according to reported statistics [2]. This was achieved despite mobile users' security and privacy concerns [3] and, most importantly, their concern over the potential disclosure of sensitive data [4,5]. Nowadays a new concern is arising, called nomophobia, due to the fear of losing smartphones along with the data stored in them [6–8]. At the same time, the growth of the Internet of Things (IoT) triggers a growth in the number of device connections, which entails that in the years to come, a vast number of connected devices must be protected [9].

To overcome these concerns, smartphone vendors implement authentication measures, such as passwords, PINs, and physiological biometrics (e.g., fingerprints, face recognition, etc.) to ensure that devices are used by legitimate users. The adoption rate of physiological biometrics has raised from 9% to 20% during the decade 2000–2010 [10]. Although these measures do provide increased security and privacy, one of their major limitations is that they authenticate users just once, when they connect to a mobile service [11]. Thus, if a smartphone gets stolen or lost while the user was logged in a service, the person who found or stole the smartphone can have access to the data stored in it. It has been shown that a password or PIN on its own is insufficient to provide adequate security for smartphones [4,12–14]. To meet this challenge, new technologies that provide continuous authentication, such as Behavioral Biometric Continuous Authentication (BBCA), face detection, have been introduced [15–19].

BBCA has emerged as a combination of Behavioral Biometrics and Continuous Authentication. BBCA is an indirect method of validation of a legitimate user based on the capture of behavioral attributes using tools and built-in smartphone sensors [20]. Behavioral biometrics refer to the observable behavior used to identify or confirm the identity of an individual. In contrast to physiological biometrics, it focuses on behavior patterns instead of physical characteristics, such as fingerprints and facial features [21]. Continuous authentication offers a safer and more protective alternative [22], and behavioral biometrics, which are incorporated within the continuous authentication framework, constitute a preferable solution for the protection of users' data [23]. In addition, a large corpus of research has shown evidence regarding the superiority of the fusion of multimodal biometric approaches. A variety of combinations is used with the fusion of biometrics that achieves improved results compared to the single modality methods [15,24,25]. Thus, the fusion of multimodal biometrics authentication emerges as a definite future trend. Hence, we consider BBCA as an effective protective technology for smartphones users.

Although a significant volume of research on BBCA has been published, the focus of recent BBCA research lies almost exclusively on the development and the improvement of behavioral biometrics continuous authentication systems [26]. On the other hand, the role of users' attitude towards BBCA technology has been overlooked. We argue that it is important to investigate the attitudes of people towards new mobile security services and explore whether factors that contribute to the usability of BBCA affect users' attitude towards these services [27]. Specifically, the following research question has guided this study: What factors affect the intention of smartphone users to use BBCA technologies?

This research intends to examine the factors associated to BBCA adoption, revealing the fundamental elements that motivate people's decisions and behavior towards this technology. To achieve this, we have built and validated a conceptual model using key elements of the Protection Motivation Theory (PMT) along with constructs that derive from the current literature related to biometrics authentication and have conducted an online survey. The survey questionnaire focuses on the identification of elements that motivate users to adopt BBCA. This work endeavors to provide a comprehensive overview of users' perspectives towards the booming BBCA applications.

The structure of this paper is as follows. In Section 2, we analyze Behavioral Biometrics Continuous Authentication technologies, mainly from the users' point of view, while Section 3 focuses on related work. In Section 4, we present the theoretical background and the research model of this work. Subsequently, in Section 5 we present the survey results, which are further discussed in Section 6. In Section 7, we consider the implications and the limitations of our research, as well future research directions, and finally conclusions are given in Section 8.

2. Background: Behavioral Biometrics Continuous Authentication

Behavioral Biometric Continuous Authentication (BBCA) is a security enhancing technology, operating alongside with the initial login process, that monitors user's behavior and continuously re-authenticates users throughout a session. BBCA is based on behavioral modalities, such as walking gait, touch gestures, keystroke dynamics, hand waving, user profile, and power consumption [15]. According to Abuhamad et al. [20], behavioral biometrics are classified into five major categories: gait, motion, voice, keystroke dynamics, and gesture. Moreover, [20] argues that a multi-modal user authentication can be provided by combining these modalities.

According to [28], 70 million smartphones are lost each year, while only 7 percent are recovered. Further to this, article [23] argues that intruders can illegally gain access to personal information if the password is compromised or if users do not maintain adequate attention to the smartphone after the initial authentication. The authors of [29] proposed as a remedy to this issue that the device should continuously monitor and validate the user after the initial login process. Schaffer [22], emphasizes that continuous authentication methods could provide a more effective means of authenticating mobile devices' users. In addition, articles [21,30] support the claim that users' authentication based on both Behavioral Biometrics (BB) and Continuous Authentication (CA) can provide high accuracy of authentication.

Currently, smartphone vendors implement both physiological biometrics and knowledge-based schemes as the primary security mechanism for identifying a user [20]. Knowledge-based approaches depend on something the users know (e.g., PINs, password, etc.), while physiological biometrics approaches depend on users' unique physiological characteristics (e.g., fingerprint, face recognition, iris). Article [11] argues that PIN-based authentication in smartphones is neither sufficient nor convenient in most situations. This drawback refers mostly to the entry-point authentication method, i.e., the authentication that takes place when a user starts a new session [22]. In addition, [20] argues that both these methods can provide point-of-entry authentication, but they fall short on delivering tacit continuous authentication, without causing constant annoyance or inconvenience to users. Another shortcoming is that physiological biometrics are mostly hardware-dependent, which increases the cost of devices [31]. On the contrary, a strong argument in favor of behavioral biometrics technology is that it can support continuous and passive authentication without depending on extra hardware [32]. Thus, behavioral biometrics have a stronger potential to fulfill the requirements for an effective authentication method [15].

Crawford, Renaud and Storer [33] report that 90% of the participants in the sample of their study are in favor of behavioral biometrics-based authentication, which reflects an increasing attention on behavioral biometrics. The authors also demonstrate that 30% of the sample do not use any security method on their smartphone, although they believe that their device should be protected. Further to this, several government projects aim to develop authentication systems based on behavioral biometrics. The US government has launched a pilot project to use behavioral biometrics for the authentication systems of the Internal Revenue Service (IRS) [9]. Also, the US Defense Information System Agency substituted employees' ID cards with a mix of behavioral biometrics and traditional measures [9]. Hence, both individual users and government organizations demonstrate an increased interest in behavioral biometrics. Despite that, however, there is a slow diffusion of behavioral biometrics pointing out that attention on protection measures usefulness is not an adequate motivation for adopting the technology. Reference [34] argues that even though technologies are available and accessible, they are nevertheless not often used. This is further supported by findings that despite evidence of government support, technologies have not been effectively diffused [35].

Although users are aware of the dangers and the existing coping technologies, they often fail to protect themselves [36,37]. Further to this, article [38] argues that there is no widespread adoption of usable technologies, such as behavioral biometrics. An

explanation of this is provided by [39]; they claim that users' behavior and decisions are guided by their mental models, so it is important for designers and developers to know and understand users' models when implementing and designing security mechanisms. Chen and Li [40] revealed that few studies have examined the motivational factors that may predict the privacy and security behavior of smartphone users. Considering all the above, we argue that it is important to identify the factors that influence individuals' intention to use BBCA technologies. Knowing these factors, BBCA systems developers would be able to improve the design of their systems so that people would be more willing to use them.

3. Related Work

Over the last two decades, several studies and reviews of continuous authentication technologies have been conducted, addressing two main topics: The first one involves the attitudes of users towards authentication, in general. Research [41] examined 175 users to investigate the adoption of continuous authentication and found that 85% of the participants believed that users should be aware of the ongoing monitoring in their devices. This revealed the importance of privacy regarding the implementation of an authentication process. The researchers also argued that the use of continuous monitoring is generally effective. Besides that, the above authors argued that some users are not comfortable with the transition to novel authentication techniques, such as continuous authentication. They also found that voice verification and fingerprint recognition were classified as the most suitable types of login authentication after passwords, with raw overall acceptability scores of 68% and 67%, respectively, indicating the growing, at the time, acceptance of biometrics.

As smartphone use started to boost, a second, more focused, topic drew the interest of security researchers. This topic concerns the attitudes and perceptions of smartphone users towards biometrics-based continuous authentication, investigating at the same time the limiting and facilitating factors affecting the adoption of these technologies. Research [42] investigated the perspectives and attitudes towards continuous authentication versus common point-of-entry authentication techniques and found that users' perspectives and attitudes varied significantly. They argued that the main justification for the negative perspectives was the fear of uncomfortability generated by false rejections. Participants also demonstrated greater concern to privacy about biometric data processing and about being continuously monitored without being aware of it.

A usability survey by [43] explored the perception of users regarding physiological and behavioral authentication methods, both of which involve active smartphones' interactivity. The results demonstrated that 87.3% of 331 attendees acknowledged that biometric authentication would be appropriate for the security of their smartphones. Also, 78.9% of the attendees agreed that they would store more private data on their devices if they were equipped with biometrics scanning features. Additionally, 66.2% of the attendees favored fingerprint as an authentication method, whereas 6.43% favored voice recognition. Research [44] found that face and hand recognition seem to be far more comfortable and lead to an enhanced perception of security in comparison to gesture and voice recognition.

Additionally, research [45] found that the combined use of different modalities had an average accuracy of 88% while 15% EER was achieved. This is in alignment with the [46] study in which the authors argued that the development and use of biometric authentication, physical as well as behavioral, in smartphones enhance their performance, security, and ease of use without major hardware side-effects that can affect and increase the price of smartphones. Further to this, article [33] argued that behavioral biometrics decrease the need for legitimate authentication by 67% compared to knowledge-based techniques. Reference [47] argued that technologies that use behavioral biometrics to provide continuous authentication on smartphones are effective since their findings among 37 participants showed that 91% found the technology suitable while 81% of them

considered the level of protection provided as sufficient. In fact, in [48], it is argued that users are amenable to adopt continuous authentication mechanisms for their smartphones. Finally, article [31] recommended BBCA as an appropriate security measure in the IoT era, since conventional methods of authentication suffer from major drawbacks, such as vulnerability and obtrusiveness.

While the aforementioned studies investigate users' perceptions towards either continuous authentication or biometrics, there is a lack of contemporary studies that address the perceptions towards their combination in BBCA. This is the first time, to our knowledge, that PMT is employed in this context. Therefore, the investigation of the factors motivating users to use BBCA is an open and important issue. Our study aspires to address this gap.

4. Theoretical Background and Research Model

In order to predict users' intention to use BBCA technology our theoretic model draws on Protection Motivation Theory along with the constructs of innovativeness, technology trust, and privacy concerns, Figure 1.
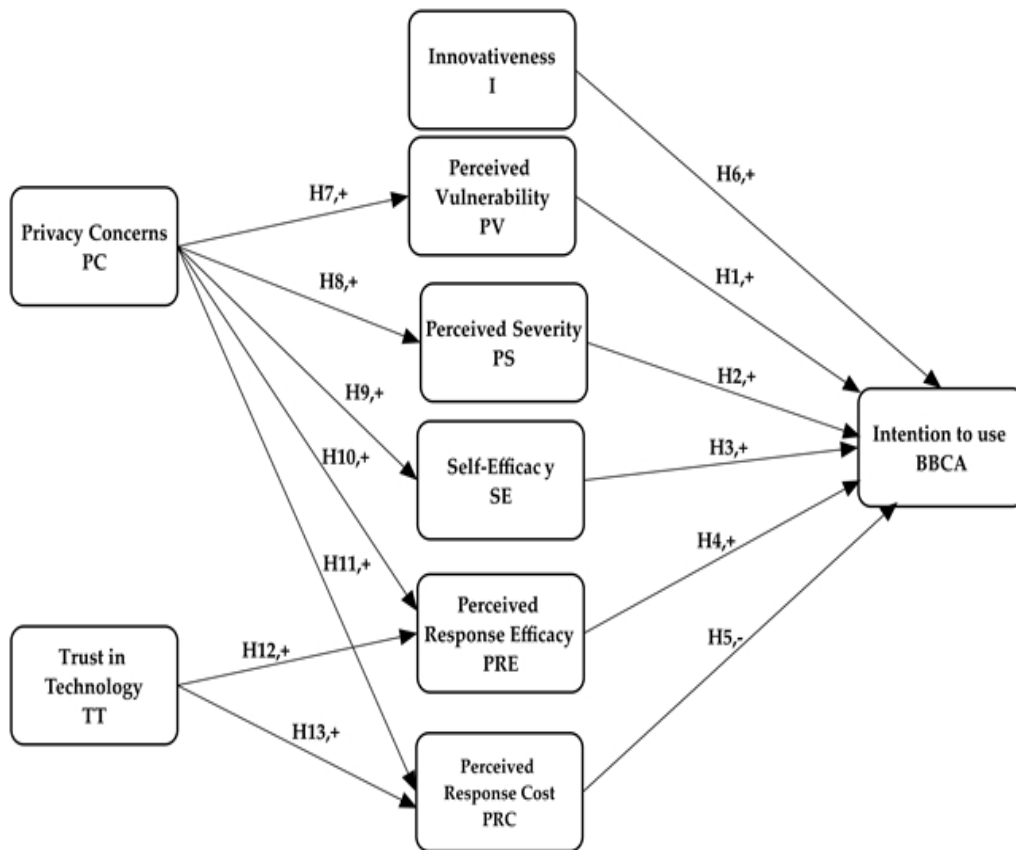

Figure 1. Research model.

Protection Motivation Theory (PMT) illustrates the way that people are motivated to react to health threats or risky behaviors, so named fear appeals [49]. Once these fear appeals arise, individuals use cognitive processes to interpret them in order to evaluate their own threat response [50].

A comprehensive literature review on PMT [51] pointed out that PMT was applied to a variety of topics of research, encompassing fields of interest other than health issues. Besides health issues and disease prevention, PMT has been extended to environmental concerns as well as privacy and security concerns, political issues, and others. The

motivation concept of protection therefore covers any threat for which the individual can respond effectively [52].

Two cognitive mediating processes are used in PMT; the threat-appraisal and the coping-appraisal process, and two types of behavior are considered; the adaptive and the maladaptive. While adaptive behaviors are acts taken by an individual for self-protection, maladaptive behaviors are purposefully avoidance reactions in response to a fear appeal. Maladaptive behavior is a behavior that is not protective against the danger generated by the fear appeal [49,52,53]. Threat appraisal estimates the consequences of maladaptive behavior and comprises three elements: severity, vulnerability (the perceptions of threat), and maladaptive rewards (intrinsic and extrinsic) [52].

Coping-appraisal assesses the ability to handle the threat and prevent it. Coping-appraisal comprises three factors: Self-efficacy, Response efficacy (efficacy variables), and Response costs. Self-efficacy is the person's perceived ability to perform the adaptive response [52]. Perceived response efficacy is the faith that the adaptive response will be successful, that protecting action will indeed be efficient in protecting oneself or others. Response costs are all costs regarding the adoption of adaptive coping response.

Although the threat appraisal component of the PMT consists of three components as indicated, for the purposes of this study only perceived vulnerability and perceived severity are used. This rests on the argument that a unified construct of response costs and rewards can be achieved since the value of risk behavior and the cost of implementing prevention measures is conceptually difficult to distinguish [54]. This explains why several PMT researches did not include response costs and rewards in the same model when investigating behaviors in informational privacy and security [55–58]. Reference [59] argues that Protection Motivation Theory (PMT) demonstrates strong explanatory power and, thus, is a valuable method for explaining precautionary online behavior. However, several researchers have challenged this argument. For instance [60] states that social cognition models such as the PMT are problematic due to the vague nature of their constructs and cannot be tested since they focus more on analytic and rather than synthetic truths. On the contrary, previous research that has used PMT revealed the effectiveness of PMT to predict individuals' security behaviors regarding internet usage [57], both via computers [61], and smartphones [58].

With the inclusion of biometric authentication in modern smartphones, privacy protection has become increasingly important in securing user biometrics [62]. Being based on personal traits, whether physiological or behavioral, biometric systems erase certain privacy issues considering their use. Mainly these issues are:

- Biometrics can be collected or shared without the permission of the specific user, without adequate knowledge, or without a specific purpose [63].
- Biometric data collected for one purpose may be used for an unintended or unauthorized purpose in the future [63].
- Biometrics can be used for purposes other than those explicitly stated, or biometrics can be abused to generate extra information [63].
- Individuals can be identified or tracked by biometrics. Since biometric data is considered unique, it can be used to track and locate persons when they try to get access to certain facilities or as their biometric attributes are collected by a surveillance system [63].
- Biometrics can be stored and/or transmitted incorrectly so they are outside the control of the user. External attacks against biometrics would be possible as a result of this [64].
- The potential threat to users' privacy posed by the misuse of biometric information is a topic of debate and frequently prevents the widespread adoption of biometric systems [63].
- Biometrics cannot be protected via conventional encryption due to their fuzzy nature. As a consequence, they are vulnerable to a variety of threats [62].

It is worth noting that determining the "true" risk of privacy violation requires taking into account a variety of factors including the factors that affect users' intention to use BBCA technologies. Given the above debate, we focus on the privacy issues of individual smartphone users, the risks they view as reasonable, and their effect on the intention to use BBCA as a self-protective behavior.

4.1. Threat-Appraisal

Threat appraisal illustrates an individual's risk assessment of a dangerous incident [65,66]. In the context of our study threat appraisal consists of the following two constructs: perceived vulnerability and perceived severity.

Perceived vulnerability refers to the likelihood that somebody might become the target of an unexpected event (i.e., a data breach incident) [50]. In our study, perceived vulnerability indicates users' appraisal of whether they are vulnerable to information security threats if no measures are taken to prevent them.

Various studies [50,66–68] demonstrate that perceived vulnerability has a major impact on coping reactions and also that people that perceive vulnerability to be high show a stronger intention to follow coping recommendations. Therefore, we hypothesize that:

Hypothesis 1 (H1). *Perceived vulnerability positively affects users' intention to use BBCA technology.*

Perceived severity is the degree to which an individual considers the consequences of an unexpected event to be severe. Article [69] argued that if an individual perceives a threat to be severe, he/she will be probably inclined to take some action. Thus, security behavior and perceived severity are linked together. Therefore, we hypothesize that:

Hypothesis 2 (H2). *Perceived severity positively affects users' intention to use BBCA technology.*

4.2. Coping-Appraisal

The process of coping-appraisal assesses the capability to cope with a threat and prevent it. Factors encompassing the process of coping are efficacy variables (self-efficacy and perceived response efficacy) and perceived response cost [52].

Self-efficacy is the person's perceived capability to perform the adaptive response. Self-efficacy in the context of our study is defined as users' belief in their ability to protect data stored in their smartphones from unauthorized disclosure, erasure, modification, destruction, and lack of availability. Self-efficacy has been discovered to have a significant illustrative impact on both technological usage and cybersecurity behavior in respect to personal information security practices [70]. Considering the above, we hypothesize that:

Hypothesis 3 (H3). *Self-efficacy positively affects users' intention to use BBCA technology.*

Perceived Response efficacy refers to the perception that the adaptive response will be effective. In the context of our research, Perceived Response efficacy refers to the users' belief that using BBCA technology will effectively protect their data. Thus, we hypothesize that:

Hypothesis 4 (H4). *Perceived Response efficacy positively affects users' intention to use BBCA technology.*

As mentioned above, some users are not comfortable with the concept of continuous monitoring. Another common issue raised against the use of continuous authentication technologies concerns power consumption. In the context of our research, we consider that users may perceive as a response cost the possibility to get lower quality of services

by their smartphones if they decide to adopt BBCA. Thus, perceived response costs are all costs regarding the adoption of adaptive coping response (e.g., financial, time, effort). In this research, we argue that users would express stronger intentions to adopt BBCA, if they consider the costs of performing protective behaviors to be low.

Therefore, we posit the following hypothesis:

Hypothesis 5 (H5). *Response costs negatively affect users' intention to use BBCA technology.*

4.3. Innovativeness

Personal innovativeness, according to [71], is important for examining the acceptance of information technology innovation. They defined personal innovativeness as the individual's willingness to experiment with any new information technology. They claim that a highly innovative person could be risk-seeking or an early adopter. Consequently, personal innovativeness influences the user's behavior or intention to use the new technology. Additionally [72] argues that security tools are what Rogers [73] names a preventive innovation. These innovations are technologies such as BBCA, that eliminate the risks of future unwanted consequences. Therefore, in the context of PMT, innovativeness is also found to be a key factor in determining the way that new technologies are adopted. Indeed, as stated in Innovation Diffusion Theory [49], the ability of an individual to try and consider new things is closely linked to the acceptance of innovative technology. Consequently, we hypothesize:

Hypothesis 6 (H6). *Innovativeness positively users' intention to use BBCA technology.*

4.4. Privacy Concerns

As computers have become so prevalent in daily life and there is a huge amount of data stored on computer devices, privacy and security have evolved into public concern [74]. Hence, the notion of informational privacy has been spotlighted in many disciplines as a key research topic, including justice, marketing, economics, psychology, and particularly in the Information Systems discipline [3]. The idea that privacy concerns relate to protective behavior is grounded in [75] who proposed that people try to use behavior strategies to achieve desired levels of privacy. Extensive research indicates that information privacy concerns are strong predictors of risk beliefs and trust in the context of electronic commerce [76] as well as the antecedents of protective behavior to disclose Internet personal information [77]. Also, privacy concerns are positively related to privacy protection, and those worried about their online privacy prefer to follow behaviors that regulate their disclosure and online privacy risks [78–80]. Further to this, many theories and studies argue that users adopt protective behaviors, if they feel they are endangered and/or if the risk is considered severe. Also, we may expect that people who are concerned about their privacy may feel more vulnerable to privacy threats and they may perceive the consequences of privacy violations to be more severe. Based on the above, we propose the following hypotheses:

Hypothesis 7 (H7). *Privacy concerns positively affect perceived vulnerability.*

Hypothesis 8 (H8). *Privacy concerns positively affect perceived severity.*

We also expect that people who are concerned about privacy may be more willing to learn how to use technologies that provide protection, such as BBCA technologies, and may perceive their efficacy to use these technologies to be high.

Hypothesis 9 (H9). *Privacy concerns positively affect self-efficacy.*

Privacy was demonstrated as a core value that drives users to adopt a protective behavior [81]. In order to apply protective behavior, users should have faith in the specific protective behavior's ability to protect them from the threat. We may expect that when users are concerned about their privacy, they may have a more positive view of protective technologies and, consequently, they may perceive their efficacy to be higher. Thus, we hypothesize:

Hypothesis 10 (H10). *Privacy concerns positively affect perceived response efficacy.*

Response cost includes the inconvenience caused by the use of extra protective technology, i.e., (BBCA), as well as the perceived cost of behavioural biometrics data collection. The latter is directly associated with the privacy concerns of the user. If users are concerned about their privacy, they may also be worried that the BBCA tool may misuse their personal data. Thus, we hypothesize that:

Hypothesis 11 (H11). *Privacy concerns positively affect perceived response cost.*

4.5. Trust

In the context of research focusing on the adaptation of innovative emerging technologies by society, technology trust is particularly essential [82]. Thus, trust in the context of our research is defined as the degree of trust that users have in technology providers, in terms of whether the services/applications they provide effectively protect their private data. Vance et al. [83] demonstrate that the degree of trust (or the lack of it) in the IT artifacts is probable to influence the intention of users to accept or not the IT artifact. Furthermore, trust, defined as the belief that personal information given to the provider will be handled securely and safely, contributes to the willingness to share personal information positively [80,84]. Having in mind this debate, we hypothesize that:

Hypothesis 12 (H12). *Trust positively affects perceived response efficacy.*

Trust is considered to associate with response cost through the concept of least effort to accomplish a task [85]. Thus, in the context of our study, this means that while the degree of trust is getting greater, the perceived response cost is getting lower. So, we hypothesize that:

Hypothesis 13 (H13). *Trust negatively affects perceived response cost.*

4.6. Survey Instrument

The survey instrument is presented in detail (see Appendix A Table A1). Whenever feasible, the items were adapted from previously validated instruments. All items were measured on a 7-point Likert scale from 1 (strongly disagree) to 7 (strongly agree). The questionnaire was developed and pre-tested among four researchers to determine the instrument's face validity. It then was pilot tested with 18 individuals from the target population. The participants were recruited from multiple areas of undergraduate and postgraduate computer engineers' school. Questions have been added, omitted, or modified based on this pilot. Finally, we recruited 778 individuals through MTurk as our research sample to complete our survey.

5. Results

In this section, we present the descriptive analysis and results of our research.

5.1. Descriptive Analysis

The sample of our research consists of 778 individuals from Europe (Germany, France, United Kingdom, Spain, Italy, Greece, Cyprus), the USA, and Asia. The

respondents were from 18 to 65 years old, 62.6% were male, while 37.4% were female. Moreover, 63.1% of respondents hold a Bachelor's degree, 30.6% a Master's degree, while 1.2% hold a Ph.D. 2% have completed Secondary Education, and 4.3% hold a Higher National Diploma. Of our sample, 38.9% were employers or entrepreneurs with salaried employees, 18% were employed, 30.1% were self-employed, 4.5% were employers or entrepreneurs without employees, 4.4% were university students, 1.6% were unemployed, and 1.6 were retired.

5.2. Measurement Model

The Kolmogorov–Smirnov's test ($p < 0.01$) showed that there is no normal distribution in all items of the model. As a result, the partial least squares (PLS) method was used as the most adequate method [86–88]. Also, to test the research hypotheses, we applied the bootstrapping method and used SmartPLS version 3.0 for the analysis [89].

Model estimation was the initial stage in data analysis. An evaluation of the internal consistency as well as discriminant validity of the instrument items are included in the measurement model test. To ensure validity, a test's internal consistency should be validated before it can be used for study or examination. Internal consistency refers to the extent to which all of the items in a test measure the same notion or construct and is thus linked to the test's interrelatedness [90].

In this study we use three measures to validate internal consistency:

- Composite reliability (CR) estimations generate an internal consistency reliability coefficient based on the proportion of variation explained by the test items compared to the overall variance of the composite test score [91].
- AVE is the average amount of variance in observed variables that a latent construct is able to explain. It is required to have an AVE of 0.5 [92,93].
- Cronbach's alpha was introduced by Lee Cronbach in 1951 [94] to provide a measure of a test's internal consistency; it is expressed as a number between 0 and 1 [94].

Thus, we examined internal consistency via composite reliability (CR) in Figure 2, the average variance (AVE) in Figure 3, and Cronbach's alpha in Figure 4. Values were all above the threshold of 0.60 (ranged from 0.700 to 0.909). The AVE values vary within the limits of 0.625 to 0.822, CR values ranged from 0.833 to 0.936, everything well above the minimum recommended of 0.50 and 0.70, respectively. Table 1 shows the factor loadings for each construct (27 in total), which all exceed the recommended value of 0.70.
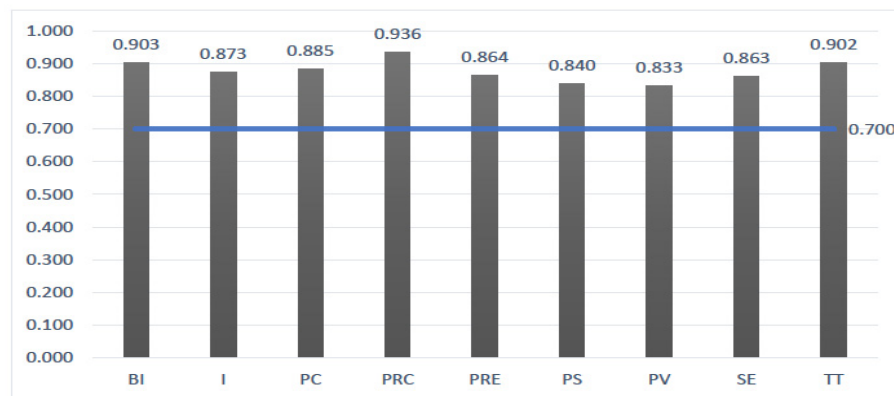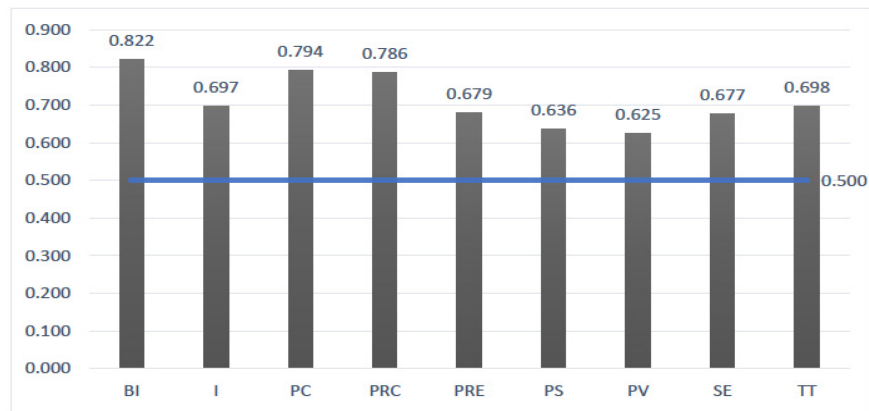

Figure 2. Composite Reliability.

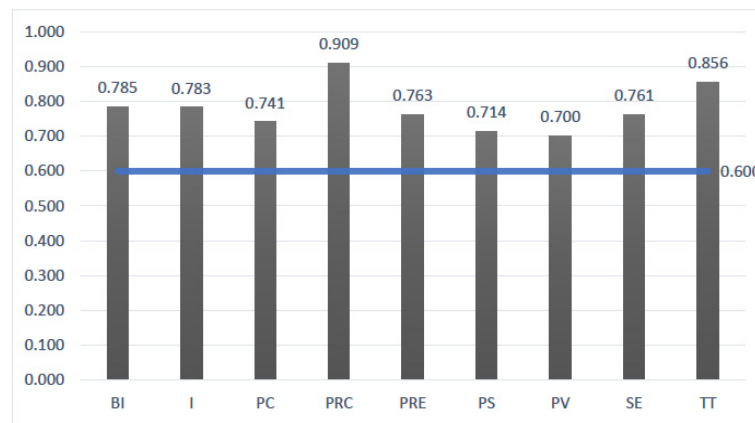**Figure 3.** Average Variance Extracted (AVE).

Figure 4. Cronbach's Alpha.

Table 1. Measurement.

Construct	Item	Mean	Std. Dev.	Factor Loadings
Innovation	I1	5.49	1.31	0.875
	I2	5.53	1.28	0.825
	I3	5.66	1.19	0.803
Privacy Concern	PC1	5.40	1.39	0.907
	PC2	5.67	1.29	0.874
Trust in Technology	TT1	5.52	1.28	0.866
	TT2	5.66	1.18	0.805
	TT3	5.52	1.29	0.829
	TT4	5.61	1.17	0.841
Perceived Vulnerability	PV1.	5.65	1.24	0.843
	PV2	5.51	1.35	0.746
	PV3	5.59	1.32	0.781
Perceived Severity	PS1	5.59	1.27	0.817
	PS2	5.57	1.34	0.789
	PS3	5.18	1.52	0.786
Self-Efficacy	SE1	5.31	1.34	0.861
	SE2	5.42	1.32	0.766
	SE3	5.35	1.32	0.839
Perceived Response Efficacy	PRE1	5.42	1.28	0.855

	PRE2	5.60	1.19	0.781
	PRE3	5.29	1.40	0.835
Perceived Response Cost	PRC1	4.57	1.79	0.920
	PRC2	4.70	1.76	0.877
	PRC3	4.61	1.79	0.901
	PRC4	4.87	1.62	0.846
Behavioral Intention	BI1	5.40	1.36	0.917
	BI2	5.49	1.33	0.897

Discriminant validity was examined to determine whether the AVE square root of each construct was greater than its highest correlation with any other construct, and the results demonstrated that there is no discriminant validity issue in the data (see Figure 5).

	BI	I	PC	PRC	PRE	PS	PV	SE	TT
BI	0.907								
I	0.734	0.835							
PC	0.192	0.258	0.891						
PRC	0.226	0.214	0.228	0.886					
PRE	0.805	0.678	0.264	0.26	0.824				
PS	0.47	0.478	0.456	0.316	0.533	0.798			
PV	0.395	0.477	0.583	0.255	0.483	0.696	0.791		
SE	0.582	0.514	0.242	0.301	0.605	0.451	0.408	0.823	
TT	0.796	0.701	0.244	0.115	0.802	0.484	0.476	0.586	0.835

Figure 5. Discriminant validity (diagonal values show AVE square root).

5.3. Structural Model Results and Hypotheses Testing

Respondents answered Likert-scale questions on which we applied one-sample t-tests. The results are presented in Table 2 showing the t-values for each correlation between the variables. For each correlation, we are interested primarily in three values: Direct effects β, t-value, and *p*-value. The t is interested in being greater than 0, and $p <= 0.05$. In the case where we have an indirect effect in BI, then for each correlation, we are interested primarily in three values: specific indirect effects β, t-value, and *p*-value.

Table 2. Direct effects, total indirect, and total effects β of determinants of intention to use BBCA technology.

Path	Direct Effects β	t-Value	R²	Hypothesis Confirmations
Behavioral Intention (BI)			0.724	
H1: Perceived Vulnerability (PV)	−0.100	3.193		Not Supported
H2: Perceived Severity (PS)	0.046	1.261		Rejected
H3: Self-Efficacy (SE)	0.103	3.273		Supported
H4: Perceived Response Efficacy (PRE)	0.532	13.735		Supported
H5: Perceived Response Cost (PRC)	−0.007	0.275		Supported
H6: Innovativeness (Innov)	0.347	9.676		Supported
Perceived Vulnerability (PV)				
H7: Privacy Concerns (PC)	0.583	16.356	0.340	Supported
Perceived Severity (PS)			0.208	
H8: Privacy Concerns (PC)	0.456	10.463		Supported
Self-Efficacy (SE)			0.059	
H9: Privacy Concerns (PC)	0.242	5.921		Supported

Perceived Response Efficacy (PRE)			0.649	
H10: Privacy Concerns (PC)	0.073	2.673		Supported
H12: Trust in Technology (TT)	0.784	35.674		Supported
Perceived Response Cost (PRC)				
H11: Privacy Concerns (PC)	0.213	4.904		Supported
H13: Trust in Technology (TT)	0.063	1.442	0.056	Rejected

Note: All effects are significant at $p < 0.001$ except H1 and H3 with $p = 0.001$.

Table 2 summarizes the results of the Bootstrapping estimation with 500 resamples and Figure 6 the structural model result. The model explains 72.4% of behavioral intention to use the technology's (BI).
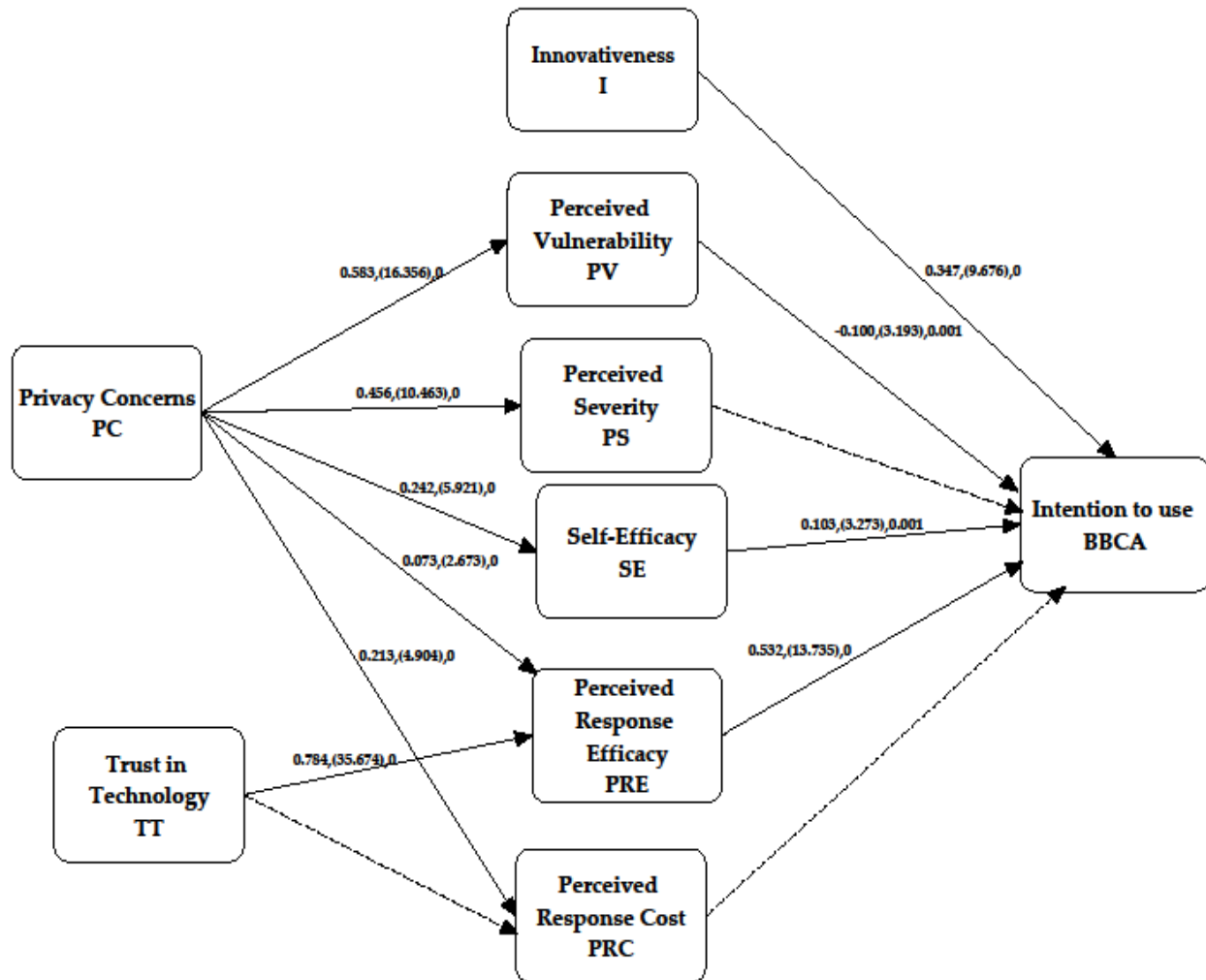

Figure 6. Structural model result. Note: in figure presented direct effects β, (t-value) and *p*-value. The dotted lines are non-significant.

Hypothesis 1 suggests that there is a positive relationship between Perceived Vulnerability (PV) and intention to use BBCA technology. No support was found for this relationship (b = −0.100; *p* > 0.01). Thus, Perceived Vulnerability (PV) works as an inhibitor in intention to use BBCA technology. This finding is in consistence with prior studies that argue [63] that the potential harm to users' privacy posed by the misuse of biometric data is a topic of debate and it frequently discourages large-scale adoption of biometric

systems. Hypothesis 2 suggests a positive relationship between perceived severity and intention to use BBCA technology. This hypothesis is not supported (b = 0.046; *p* > 0.01). This result is consistent with some prior research works [95], but not all [48]. Thus, this evidence provides mixed findings on perceived severity.

Hypothesis 3 proposes a positive relationship between self efficacy and intention to use BBCA technology. Self-efficacy, as hypothesized, contributes positively to intention to use BBCA technology. This is consistent with prior studies that argue that people who have a high degree of self-efficacy have a greater sense of self-belief in their ability to mobilize motivation, and courses of action required to complete a mission successfully [93]. Consistent with prior studies [69], our study found that users who have a stronger confidence in the availability of information security technologies and procedures, in general, have expressed greater belief in their ability to manipulate personal threats to information security. Hypothesis 4 suggests a positive relationship between Perceived Response Efficacy (PRE) and users' intention to use BBCA technology. Perceived Response Efficacy (PRE) contributes positively to Privacy Concerns (PC) (b = 0.532; *p* < 0.01); thus supporting Hypothesis 4. This is consistent with current research, which has found that response effectiveness is one of the strongest predictors of behavioral outcomes related to information security [95,96]. Hypothesis 5 proposes a negative relationship between response costs and intention to use BBCA technology. Response costs (b = −0.007; *p* < 0.01) as hypothesized works as an inhibitor to the intention to use BBCA technology, which is aligned with prior studies [49]. Hypothesis 6 proposes a positive relationship between innovativeness and users' intention to use BBCA technology. Innovativeness contributes positively to users' intention to use BBCA technology (b = 0.347; *p* < 0.01); thus supporting Hypothesis 6. This is in alignment with [70] that found that the acceptance of innovative information technologies by their intended users is an important issue for both users and practitioners.

The model of our study explains 34% of Perceived Vulnerability (PV) and 20.8% of Perceived Severity (PS), as both H7 and H8 are supported. Hypothesis 7 suggests a positive relationship between Privacy Concerns (PC) and Perceived Vulnerability (PV). Privacy Concern (PC) is a strong antecedent of Perceived Vulnerability (PV) (b = 0.583; *p* < 0.01). Also Hypothesis 8 proposes a positive relationship between Privacy Concerns (PC) and perceived severity. Privacy Concern contributes positively to perceived severity (b = 0.456; *p* < 0.01); thus supporting Hypothesis 8. Both findings are consistent with studies that claim that the level of privacy concern motivates coping behaviors to deal with privacy risks [89].

Hypothesis 9 suggests a positive relationship between Privacy Concerns (PC) and self-efficacy. Privacy concern has a positive effect on self-efficacy (b = 0.242; *p* < 0.01), thus supporting Hypothesis 9. This suggests that users' who are concerned about their privacy are more interested in learning how to use privacy-protecting technologies. This finding supports prior studies that show a significant relationship between self-efficacy and privacy concerns [52].

Hypothesis 10 proposes a positive relationship between Privacy Concerns (PC) and Perceived Response Efficacy (PRE). Privacy Concerns (PC) contribute positively to Perceived Response Efficacy (PRE) (b = 0.073; *p* < 0.01); thus supporting Hypothesis 10. This is in consistence with prior studies [7,61,65] that have found that users who have higher privacy concerns seek sufficient information about the efficacy of a suggested coping mechanisms in providing protection from a threat or danger and they are more likely to follow adaptive behavior. Hypothesis 11 suggests a positive relationship between Privacy Concerns (PC) and Perceived Response Cost (PRC). Privacy concerns has a positive effect on Perceived Response Cost (PRC) (b = 0.213; *p* < 0.01), thus supporting Hypothesis 11. Users may be concerned about their privacy, as well as the possibility that this technology will jeopardize their personal data. Hypothesis 12 suggests a positive relationship between Trust (T) and Perceived Response Efficacy (PRE). Privacy Concerns (PC) contribute positively to Perceived Response Efficacy (PRE) (b = 0.784; *p* < 0.01), thus

supporting Hypothesis 12. This is in consistence with the findings of [82] claiming that the level of trust (or lack of it) in IT artifacts affects users' decision to accept or reject the IT artifact.

6. Discussion

6.1. Privacy Concerns as Antecedent of Coping Appraisal

This study has contributed to a better understanding of information privacy concerns as a predictor of coping and threat appraisal processes, since our findings reveal that privacy concerns have a significant direct effect on both aforementioned processes. Specifically, we found that privacy concerns have a significant impact on all components of PMT. Privacy concerns, as was expected, have a positive direct effect on Perceived severity. Indeed, this research proposes that users who have higher privacy concerns, consider the consequences of the risk to be more severe than those who have lower privacy concerns. Also, privacy concerns positively affect perceived vulnerability. Both findings are in alignment with studies that argue that the level of privacy concerns motivates coping behaviors to handle privacy risks [95].

The path from privacy concerns to self-efficacy was also found to be significant. Thus, users who demonstrate high interest in privacy feel stronger confidence to use information security technologies that protect their privacy. It was also found that privacy concerns have a direct positive effect on perceived response efficacy as hypothesized. Indeed, users who have higher privacy concerns seek sufficient information about the efficacy of suggested coping mechanisms that provide protection, and they are more likely to follow an adaptive behavior.

Moreover, our findings demonstrate that privacy concerns positively affect perceived response cost. This suggests that users with high privacy concerns are worried that their behavioral biometrics, managed by the BBCA tool, could be misused. Thus, the risk of biometrics misuse (e.g., to be disclosed or to use biometric of someone for purposes other than those specified) adds to the perceived cost of using BBCA technologies.

6.2. Perceived Vulnerability

Contrary to our hypothesis, the perceived vulnerability affects the user's intention to use BBCA technologies as an inhibitor. Although this was unexpected, an important finding of our research is that users consider the BBCA itself as a potential threat. This suggests that the feeling of vulnerability against privacy threats is overlapping with the feeling of vulnerability caused by the threat of an improper behavioral monitoring tool. Therefore, we argue that users who feel vulnerable to a privacy violation hesitate to use BBCA technologies. Further to the above, this finding provides strong evidence that users emphasize the reliability and trustworthiness of security tools. This could be a very useful suggestion for BBCA tools developers.

6.3. Self Efficacy

Self-efficacy positively affects users' intention to use BBCA technology. The findings suggest that users' strong beliefs about their abilities to engage in using BBCA has an impact on their intention to use or not the technology. Users with a high level of self-efficacy are more confident in their capacity to take the steps necessary to fulfill a mission successfully. Hence, a strong sense of efficacy motivates individuals to use protective technologies, such as BBCA.

6.4. Perceived Response Efficacy

Findings also suggest that perceived response efficacy is the major facilitator in users' intention to use BBCA technology. This is in alignment with current studies that have found that response effectiveness is typically one of the strongest predictors of behavioral

outcome linked to information security [95,96]. Therefore, our study's findings emphasize the critical importance of convincing users that BBCA is an effective technology.

6.5. Innovativeness

Finally, we found that innovativeness is another important construct that affects the intention to use BBCA technologies. The supportive findings show that more innovative users are more positive towards BBCA. This suggests that the acceptance of innovative security technologies by the intended users is an important issue.

7. Implications, Limitations, and Future Research

The goal of this study is to identify the factors that motivate individuals' intention to use BBCA technology from the perspective of PMT, so that BBCA vendors can be better informed about how to develop more user-friendly tools that are more in tune with users' requirements. Our research adds to the existing body of knowledge by incorporating the constructs of privacy concerns as predictors of coping and threat appraisal processes, as well as innovativeness as a predictor of intention to use. Specifically, this research reveals the significance of privacy concerns when the Protection Motivation Theory is applied in the field of digital privacy. Regarding maladaptive coping behaviors, we provide an alternative explanation why protective information security behaviors have yet to be adopted, as users hesitate to use BBCA technologies when they feel vulnerable to potential misuse of their personal data by the same technologies that aim to protect their privacy and security. Even when people are motivated to protect themselves, the sense of vulnerability generated by the threat of an improper monitoring tool outweighs the fear of privacy threats.

Regarding practice, our findings benefit developers of BBCA technologies in developing tools that better satisfy the needs of users. Our research provides useful insights to them, revealing the need for reliable and trustworthy BBCA tools that assure users that their behavioral biometric data are safe. Most significantly, BBCA vendors need to design and promote comprehensive standards to build trust with users and ensure that BBCA tools development complies with these requirements.

While this study's results are insightful, they must be viewed in the context of certain limitations. First, since the questionary was filled out online, the study environment was less regulated. Background noise or the presence of other people in the session, for example, may have disrupted or affected participants. This implies that actions may have been influenced by factors other than the manipulated variables. It is also conceivable that some of the measurement items in the study questionnaire, as well as their wordings, might have been misinterpreted by the respondents, resulting in biased responses. Further to the above, a major drawback of the use of MTurk for academic research is the threat to external validity [16]

However, the external validity of data collected through MTurk appears to be a benefit rather than a concern, as MTurk offers a unique range of diversity in the United States and globally, which we took advantage of.

Finally, although our PMT-based model is fairly effective in predicting behavior, further research could be conducted to investigate other factors, such as ethical, social, and convenience factors, to increase its predictive power. Another approach could include situational considerations, such as current legal regulations and user's previous experience of security breaches.

8. Conclusions

In this study, we investigated the factors that affect the intention of using BBCA technology. We employed Protection Motivation Theory and enhanced our research model with constructs that derive from the extant literature. After collecting the data from our recruited sample, our statistical analysis concluded that privacy concerns towards the

intention of use BBCA technology had an important impact on all components of PMT. Further to this, another important construct that we found that affects the usage intention of BBCA technology is innovativeness. In addition:

- 72.4% of users have the intention to use BBCA technology. Among them.
- 34% will use BBCA because of Perceived Vulnerability.
- 20.8% will use BBCE because of Perceived Severity.
- 64.9% will use BBCA because of Perceived Response Efficacy.

Thus, regarding PMT, we found that users focus more on response efficacy rather than severity and vulnerability. We believe that this implies that users would use a BBCA technology that is effective and practical even if the response cost of using it is high. This is a hopeful result that makes us optimistic for the adoption of BBCA.

Appendix A. Questionnaire

Table A1. Bioprivacy Survey Instrument.

Construct	Item	Question	Adapted from
Innovativeness **I**	I1	I am among the first to try out new technologies.	
	I2	When I hear about a new technology, I look for ways to adopt it.	[97]
	I3	I like to experiment with new technologies.	[98]
	I4	I am a person who searches for novel approaches not required at the time.	
Privacy Concerns **PC**	PC1	I am concerned that my personal information could be used for wrong purposes.	[99]
	PC2	I am concerned that my personal information could be accessed by unknown parties.	
Trust in Technology **TT**	TT1	I would trust biometric authentication system.	
	TT2	I think the biometric authentication service would be reliable.	[100]
	TT3	I believe that a biometric authentication system would be employed in my best Interest.	[101]
	TT4	I feel fine using biometric authentication systems since they are generally reliable and accurate.	
Perceived Vulnerability **PV**	PV1	If my data leak while using my mobile phone, I could be vulnerable to an information security threat.	[102]
	PV2	If any data breach while using my mobile phone, my organization could be vulnerable to an information security threat.	[66]
	PV3	If the data that I keep in my phone (e.g., photos, messages) leak, then my privacy would be compromised.	Self-developed
Perceived Severity **PS**	PS1	I believe that if my personal data that I keep in my mobile phone leak, it will be harmful for me.	[103]
	PS2	A loss of my personal data from my mobile phone could cause a serious anxiety problem to me and my family.	[102]
	PS3	My lost or stolen mobile phone would bring financial or reputational loss to my company.	[104]
Self-Efficacy **SE**	SE1	I would use mobile internet technologies, including biometric authentication systems, if I had only the system manuals for reference.	[105]
	SE2	I would use mobile internet technologies, including biometric authentication systems, if I had seen someone else using it before trying it myself.	[106]

	SE3	I would use mobile internet technologies, including biometric authentication systems, if I could call someone for help if I got stuck.	
Perceived Response Efficacy PRE	PRE1	The biometric authentication measures available to me to for stopping people from getting my confidential information from my mobile phone are adequate.	[107]
	PRE2	I am confident that biometric authentication systems would be effective in keeping my data safe.	[108]
	PRE3	I am confident that the biometric authentication system will not use my personal data for other purposes.	
Perceived Response Cost PRC	PRC1	Using a biometric authentication system is too much trouble.	[103]
	PRC2	Biometric authentication system may cause problems to other programs on my mobile phone.	[109]
	PRC3	Biometric authentication system may make me loose critical information.	
	PRC4	The cost of using a biometric authentication system, including the inconvenience it might cause to me, exceeds benefits.	[107]
Behavioral Intention to accept the technology BI	BI1	I should apply this BBCA technology as soon as possible.	[110]
	BI2	I should use this BBCA technology soon after it is launched.	

References

1. Martin, T.; Karopoulos, G.; Hernández-Ramos, J.L.; Kambourakis, G.; Fovino, I.N. Demystifying COVID-19 Digital Contact Tracing: A Survey on Frameworks and Mobile Apps. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 8851429. https://doi.org/10.1155/2020/8851429.
2. Global Stats Counter. 2020. Available online:: https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/worldwide/2020 (accessed on 23 October 2021).
3. Xu, H.; Gupta, S.; Rosson, M.B.; Carroll, J.M. *Measuring Mobile Users' Concerns for Information Privacy*; Citeseer: Princeton, NJ, USA, 2012.
4. Kurkovsky, S.; Syta, E. Digital natives and mobile phones: A survey of practices and attitudes about privacy and security. In Proceedings of the 2010 IEEE International Symposium on Technology and Society, Wollongong, Australia, 7–9 June 2010; pp. 441–449. https://doi.org/10.1109/istas.2010.5514610.
5. Feng, T.; Liu, Z.; Kwon, K.A.; Shi, W.; Carbunar, B.; Jiang, Y.; Nguyen, N. Continuous mobile authentication using touchscreen gestures. In Proceedings of the 2012 IEEE Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 13–15 November 2012; pp. 451–456.
6. Yildirim, C.; Correia, A.-P. Exploring the dimensions of nomophobia: Development and validation of a self-reported questionnaire. *Comput. Hum. Behav.* **2015**, *49*, 130–137. https://doi.org/10.1016/j.chb.2015.02.059.
7. Aguilera-Manrique, G.; Márquez-Hernández, V.V.; Alcaraz-Córdoba, T.; Granados-Gámez, G.; Gutierrez-Puertas, V.; Gutiérrez-Puertas, L. The relationship between nomophobia and the distraction associated with smartphone use among nursing students in their clinical practicum. *PLoS ONE* **2018**, *13*, e0202953. https://doi.org/10.1371/journal.pone.0202953.
8. Gonçalves, S.; Dias, P.; Correia, A.-P. Nomophobia and lifestyle: Smartphone use and its relationship to psychopathologies. *Comput. Hum. Behav. Rep.* **2020**, *2*, 100025. https://doi.org/10.1016/j.chbr.2020.100025.
9. Bhattacharya, N. Behavioural biometrics in action. *Biomed. Technol. Today* **2020**, *2020*, 8–11. https://doi.org/10.1016/s0969-4765(20)30134-x.
10. Clarke, N. *Transparent User Authentication: Biometrics, RFID and Behavioural Profiling;* Springer Science & Business Media: Cham, Switzerland, 2011.
11. Ben-Asher, N.; Kirschnick, N.; Sieger, H.; Meyer, J.; Ben-Oved, A.; Möller, S. On the need for different security methods on mobile phones. In Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services, Stockholm, Sweden, 30 August–2 September 2011; pp. 465–473.
12. Clarke, N.L.; Furnell, S.M. Authentication of users on mobile telephones—A survey of attitudes and practices. *Comput. Secur.* **2005**, *24*, 519–527.
13. Ahern, S.; Eckles, D.; Good, N.S.; King, S.; Naaman, M.; Nair, R. Over-exposed? Privacy patterns and considerations in online and mobile photo sharing. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, San Jose, CA, USA, 28 April–3 May 2007; Association for Computing Machinery: New York, NY, USA, 2007; pp. 357–366. https://doi.org/10.1145/1240624.1240683.
14. Keith, M.J.; Thompson, S.C.; Hale, J.; Lowry, P.; Greer, C. Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *Int. J. Hum. Comput. Stud.* **2013**, *71*, 1163–1173. https://doi.org/10.1016/j.ijhcs.2013.08.016.
15. Stylios, I.; Kokolakis, S.; Thanou, O.; Chatzis, S. Behavioral biometrics & continuous user authentication on mobile devices: A survey. *Inf. Fusion* **2020**, *66*, 76–99. https://doi.org/10.1016/j.inffus.2020.08.021..
16. Crowston, K. *Amazon Mechanical Turk: A Research Tool for Organizations and Information Systems Scholars*; Springer: Cham, Switzerland, 2012; pp. 210–221. https://doi.org/10.1007/978-3-642-35142-6_14.
17. Sitova, Z.; Sedenka, J.; Yang, Q.; Peng, G.; Zhou, G.; Gasti, P.; Balagani, K.S. HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users. *IEEE Trans. Inf. Forensics Secur.* **2015**, *11*, 877–892. https://doi.org/10.1109/tifs.2015.2506542.
18. Mahbub, U.; Patel, V.M.; Chandra, D.; Barbello, B.; Chellappa, R. Partial face detection for continuous authentication. In Proceedings of the 2016 IEEE International Conference on Image Processing (ICIP), Phoenix, AZ, USA, 25–28 September 2016; pp. 2991–2995.
19. Abuhamad, M.; Abuhmed, T.; Mohaisen, D.; Nyang, D.H. AUToSen: Deep-Learning-Based Implicit Continuous Authentication Using Smartphone Sensors. *IEEE Internet Things J.* **2020**, *7*, 5008–5020. https://doi.org/10.1109/jiot.2020.2975779.
20. Abuhamad, M.; Abusnaina, A.; Nyang, D.H.; Mohaisen, D. Sensor-Based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey. *IEEE Internet Things J.* **2020**, *8*, 65–84. https://doi.org/10.1109/jiot.2020.3020076.
21. Stylios, I.; Thanou, O.; Androulidakis, I.; Zaitseva, E. A Review of Continuous Authentication Using Behavioral Biometrics. In Proceedings of the SouthEast European Design Automation, Computer Engineering, Computer Networks and Social Media Conference, Kastoria, Greece, 25–27 September 2016; pp. 72–79. https://doi.org/10.1145/2984393.2984403.
22. Schaffer, K. Expanding Continuous Authentication with Mobile Devices. *Computer* **2015**, *48*, 92–95. https://doi.org/10.1109/mc.2015.333.
23. Patel, V.M.; Chellappa, R.; Chandra, D.; Barbello, B. Continuous User Authentication on Mobile Devices: Recent progress and remaining challenges. *IEEE Signal Process. Mag.* **2016**, *33*, 49–61. https://doi.org/10.1109/msp.2016.2555335.

24. Buriro, A.; Crispo, B.; Del Frari, F.; Klardie, J.; Wrona, K. *ITSME: Multi-Modal and Unobtrusive Behavioural User Authentication for Smartphones*; Springer: Cham, Switzerland, 2016; pp. 45–61. https://doi.org/10.1007/978-3-319-29938-9_4.

25. Saevanee, H.; Clarke, N.L.; Furnell, S.M. Multi-modal behavioural biometric authentication for mobile devices. In *IFIP International Information Security Conference*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 465–474.

26. Stylios, I.; Skalkos, A.; Kokolakis, S.; Karyda, M. BioPrivacy: Development of a Keystroke Dynamics Continuous Authentication System. In Proceedings of the 5th International Workshop on SECurity and Privacy Requirements Engineering SECPRE, Online, 4–8 October 2021.

27. Koivumäki, T.; Ristola, A.; Kesti, M. The perceptions towards mobile services: An empirical analysis of the role of use facilitators. *Pers. Ubiquitous Comput.* **2006**, *12*, 67–75. https://doi.org/10.1007/s00779-006-0128-x.

28. Hom, E. Mobile Device Security: Startling Statistics on Data Loss and Data Breaches. 2017. Available online: https://www.channelpronetwork.com/article/mobile-device-security-startling-statistics-data-loss-and-data-breaches (accessed on 8 January 2021).

29. Prakash, A.; Mukesh, R. A Biometric Approach for Continuous User Authentication by Fusing Hard and Soft Traits. *IJ Netw. Secur.* **2014**, *16*, 65–70.

30. Shnidman, R. Biometric Authentication: The How and Why. 2017. Available online: https://about-fra ud.com/biometric-authentication (accessed on 11 January 2021).

31. Liang, Y.; Samtani, S.; Guo, B.; Yu, Z. Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective. *IEEE Internet Things J.* **2020**, *7*, 9128–9143. https://doi.org/10.1109/jiot.2020.3004077.

32. Alzubaidi, A.; Kalita, J. Authentication of Smartphone Users Using Behavioral Biometrics. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1998–2026. https://doi.org/10.1109/comst.2016.2537748.

33. Crawford, H.; Renaud, K.; Storer, T. A framework for continuous, transparent mobile device authentication. *Comput. Secur.* **2013**, *39*, 127–136. https://doi.org/10.1016/j.cose.2013.05.005.

34. Dourish, P.; Grinter, R.E.; De La Flor, J.D.; Joseph, M. Security in the wild: User strategies for managing security as an everyday, practical problem. *Pers. Ubiquitous Comput.* **2004**, *8*, 391–401. https://doi.org/10.1007/s00779-004-0308-5.

35. Alwahaishi, S.; Snásel, V. Consumers Acceptance and Use of Information and Communications Technology: A UTAUT and Flow Based Theoretical Model. *J. Technol. Manag. Innov.* **2013**, *8*, 9–10. https://doi.org/10.4067/s0718-27242013000200005.

36. Albrechtsen, E. A qualitative study of users view on information security. *Comput. Secur.* **2007**, *26*, 276–289. https://doi.org/10.1016/j.cose.2006.11.004.

37. Gerber, N.; Zimmermann, V.; Volkamer, M. Why johnny fails to protect his privacy. In Proceedings of the 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Stockholm, Sweden, 17–19 June 2019; pp. 109–118.

38. Alkaldi, N.; Renaud, K. Why do people adopt or reject smartphone security tools? In Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance, HAISA 2016, Frankfurt, Germany, 19–21 July 2016; pp. 135–144.

39. Volkamer, M.; Renaud, K. Mental models–general introduction and review of their application to human-centred security. In *Number Theory and Cryptography*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 255–280. https://doi.org/10.1007/978-3-642-42001-6_18.

40. Chen, H.; Li, W. Mobile device users' privacy security assurance behavior. *Inf. Comput. Secur.* **2017**, *25*, 330–344. https://doi.org/10.1108/ics-04-2016-0027.

41. Furnell, S.; Dowland, P.; Illingworth, H.; Reynolds, P. Authentication and Supervision: A Survey of User Attitudes. *Comput. Secur.* **2000**, *19*, 529–539. https://doi.org/10.1016/s0167-4048(00)06027-2.

42. Karatzouni, S.; Furnell, S.M.; Clarke, N.L.; Botha, R.A. Perceptions of User Authentication on Mobile Devices. In Proceedings of the 6th Annual ISOnEworld Conference, Las Vegas, NV, USA, 11–13 April 2007; pp. 11–13.

43. Alhussain, T.; Alghamdi, R.; Alkhalaf, S.; Alfarraj, O. Users Perceptions of Mobile Phone Security: A Survey Study in the Kingdom of Saudi Arabia. *Int. J. Comput. Theory Eng.* **2013**, *5*, 793–796. https://doi.org/10.7763/ijcte.2013.v5.798.

44. Guerra-Casanova, J.; Ríos-Sánchez, B.; Viana-Matesanz, M.; Bailador, G.; Sanchez-Avila, C.; De Giles, M.J.M. Comfort and security perception of biometrics in mobile phones with widespread sensors. In Proceedings of the 2016 IEEE 35th symposium on reliable distributed systems workshops (SRDSW), Budapest, Hungary, 26 September 2016; pp. 13–18.

45. Volaka, H.C.; Alptekin, G.; Basar, O.E.; Isbilen, M.; Incel, O.D. Towards Continuous Authentication on Mobile Phones using Deep Learning Models. *Procedia Comput. Sci.* **2019**, *155*, 177–184. https://doi.org/10.1016/j.procs.2019.08.027.

46. Abazi, B.; Qehaja, B.; Hajrizi, E. Application of biometric models of authentication in mobile equipment. *IFAC-PapersOnLine* **2019**, *52*, 543–546. https://doi.org/10.1016/j.ifacol.2019.12.602.

47. Khan, H.; Hengartner, U.; Vogel, D. 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, Ottawa, ON, CA, 22–24 July 2015; pp. 225–239.

48. Rasnayaka, S.; Sim, T. Who wants Continuous Authentication on Mobile Devices? In Proceedings of the 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), Redondo Beach, CA, USA, 22–25 October 2018; pp. 1–9.

49. Rogers, R.W. A Protection Motivation Theory of Fear Appeals and Attitude Change1. *J. Psychol.* **1975**, *91*, 93–114. https://doi.org/10.1080/00223980.1975.9915803.

50. Vance, A.; Siponen, M.; Pahnila, S. Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Inf. Manag.* **2012**, *49*, 190–198. https://doi.org/10.1016/j.im.2012.04.002.

51. Rogers, R.W.; Prentice-Dunn, S. Protection motivation theory. In *Handbook of Health Behavior Research 1: Personal and Socialdeterminants*; Gochman, D.S., Ed.; Plenum Press: New York, NY, USA, 1997; pp. 113–132.

52. Floyd, D.L.; Prentice-Dunn, S.; Rogers, R.W. A Meta-Analysis of Research on Protection Motivation Theory. *J. Appl. Soc. Psychol.* **2000**, *30*, 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x.

53. Milne, G.R.; Labrecque, L.I.; Cromer, C. Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices. *J. Consum. Aff.* **2009**, *43*, 449–473.

54. Abraham, C.S.; Sheeran, P.; Abrams, W.D.J.; Spears, R. Exploring teenagers' adaptive and maladaptive thinking in relation to the threat of hiv infection. *Psychol. Health* **1994**, *9*, 253–272. https://doi.org/10.1080/08870449408407485.

55. Hanus, B.; Wu, Y. Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Inf. Syst. Manag.* **2015**, *33*, 2–16. https://doi.org/10.1080/10580530.2015.1117842.

56. Ifinedo, P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Comput. Secur.* **2012**, *31*, 83–95. https://doi.org/10.1016/j.cose.2011.10.007.

57. Tsai, H.-Y.S.; Jiang, M.; Alhabash, S.; LaRose, R.; Rifon, N.J.; Cotten, S.R. Understanding online safety behaviors: A protection motivation theory perspective. *Comput. Secur.* **2016**, *59*, 138–150. https://doi.org/10.1016/j.cose.2016.02.009.

58. Verkijika, S.F. Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Comput. Secur.* **2018**, *77*, 860–870. https://doi.org/10.1016/j.cose.2018.03.008.

59. Jansen, J.; Van Schaik, P. Understanding Precautionary Online Behavioural Intentions: A Comparison of Three Models. In Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance, HAISA 2016, Frankfurt, Germany, 19–21 July 2016; Clarke, N., Furnell, S., Eds.; pp. 1–11.

60. Ogden, J. Some problems with social cognition models: A pragmatic and conceptual analysis. *Health Psychol.* **2003**, *22*, 424–428. https://doi.org/10.1037/0278-6133.22.4.424.

61. Anderson; Agarwal Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Q.* **2010**, *34*, 613. https://doi.org/10.2307/25750694.

62. Stajkovic, A.D.; Luthans, F. Self-efficacy and work-related performance: A meta-analysis. *Psychol. Bull.* **1998**, *124*, 240.

63. Campisi, P. *Security and Privacy in Biometrics: Towards a Holistic Approach*; Springer: Cham, Switzerland, 2013; pp. 1–23. https://doi.org/10.1007/978-1-4471-5230-9_1.

64. Tran, Q.N.; Turnbull, B.P.; Hu, J. Biometrics and Privacy-Preservation: How Do They Evolve? *IEEE Open J. Comput. Soc.* **2021**, *2*, 179–191. https://doi.org/10.1109/ojcs.2021.3068385.

65. Rogers, R. Cognitive and physiological processes in fear-based attitude change: A revised theory of protection motivation. In *Social Psychophysiology: A Sourcebook*; Cacioppo, J., Petty, R., Eds.; Guilford Press: New York, NY, USA, 1983; pp. 153–176.

66. Woon, I.M.Y.; Tan, G.W.; Low, R.T. A protection motivation theory approach to home wireless security. In Proceedings of the International Conference on Information Systems, ICIS 2005, Las Vegas, NV, USA, 11–14 December 2005.

67. Rippetoe, S.; Rogers, R.W. Effects of Components of Protection-Motivation Theory on Adaptive and Maladaptive Coping with a Health Threat. *J. Personal. Soc. Psychol.* **1987**, *52*, 596–604.

68. Wurtele, S.K.; Maddux, J.E. Relative Contributions of Protection Motivation Theory Components in Predicting Exercise Intentions and Behavior. *Health Psychol.* **1987**, *6*, 453–466.

69. Ng, B.-Y.; Kankanhalli, A.; Xu, Y. Studying users' computer security behavior: A health belief perspective. *Decis. Support Syst.* **2009**, *46*, 815–825. https://doi.org/10.1016/j.dss.2008.11.010.

70. Rhee, H.-S.; Kim, C.; Ryu, Y.U. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Comput. Secur.* **2009**, *28*, 816–826. https://doi.org/10.1016/j.cose.2009.05.008.

71. Agarwal, R.; Prasad, J. A Conceptual and Operational Definition of Personal Innovativeness in the Domain of Information Technology. *Inf. Syst. Res.* **1998**, *9*, 204–215. https://doi.org/10.1287/isre.9.2.204.

72. Xiao, S.; Witschey, J.; Murphy-Hill, E. Social influences on secure development tool adoption: Why security tools spread. In Proceedings of the 17th ACM conference on Computer Supported Cooperative Work& Social Computing, Baltimore, MD, USA, 15–19 February 2014; pp. 1095–1106.

73. Rogers, E.M. *Diffusion of Innovations*; Simon and Schuster: New York, NY, USA, 2010.

74. Ware, W.H. *Records, Computers, and the Rights of Citizens: Report*; US Department of Health, Education & Welfare: Washington, DC, USA, 1973; Volume 10.

75. Gove, W.R. Review of the Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding., by I. Altman. *Contemp. Sociol.* **1978**, *7*, 638–638. https://doi.org/10.2307/2065073.

76. Malhorta, N.K.; Kim, S.S.; Agarwal, J. Internet users' information privacy concerns (IUIPC): The construct, the scale and a causal model. *Inf. Syst. Res.* **2004**, *15*, 336–355.

77. Son, J.Y.; Kim, S.S. Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Q.* **2008**, *32*, 503–529.

78. Sheehan, K.B.; Hoy, M.G. Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns. *J. Advert.* **1999**, *28*, 37–51. https://doi.org/10.1080/00913367.1999.10673588.

79. Youn, S.; Hall, K. Gender and Online Privacy among Teens: Risk Perception, Privacy Concerns, and Protection Behaviors. *Cyber Psychol. Behav.* **2008**, *11*, 763–765. https://doi.org/10.1089/cpb.2007.0240.

80. Chen, H.-T.; Chen, W. Couldn't or Wouldn't? The Influence of Privacy Concerns and Self-Efficacy in Privacy Management on Privacy Protection. *Cyber Psychol. Behav. Soc. Netw.* **2015**, *18*, 13–19. https://doi.org/10.1089/cyber.2014.0456.

81. Skalkos, A.; Tsohou, A.; Karyda, M.; Kokolakis, S. Identifying the values associated with users' behavior towards anonymity tools through means-end analysis. *Comput. Hum. Behav. Rep.* **2020**, *2*, 100034. https://doi.org/10.1016/j.chbr.2020.100034.

82. Ejdys, J. Building technology trust in ICT application at a university. *Int. J. Emerg. Mark.* **2018**, *13*, 980–997. https://doi.org/10.1108/ijoem-07-2017-0234.

83. Vance, A.; Elie-Dit-Cosaque, C.M.; Straub, D.W. Examining Trust in Information Technology Artifacts: The Effects of System Quality and Culture. *J. Manag. Inf. Syst.* **2008**, *24*, 73–100. https://doi.org/10.2753/mis0742-1222240403.

84. Krasnova, H.; Veltri, N.F.; Günther, O. Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture. *Bus. Inf. Syst. Eng.* **2012**, *4*, 127–135. https://doi.org/10.1007/s12599-012-0216-6.

85. Hertzum, M. The importance of trust in software engineers' assessment and choice of information sources. *Inf. Organ.* **2002**, *12*, 1–18. https://doi.org/10.1016/s1471-7727(01)00007-0.

86. Miltgen, C.L.; Popovič, A.; Oliveira, T. Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context. *Decis. Support Syst.* **2013**, *56*, 103–114. https://doi.org/10.1016/j.dss.2013.05.010.

87. Chin, W.W.; Marcolin, B.L.; Newsted, P.R. A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion/Adoption Study. *Inf. Syst. Res.* **2003**, *14*, 189–217. https://doi.org/10.1287/isre.14.2.189.16018.

88. Hair, J.F., Jr.; Hult, G.T.M.; Ringle, C.; Sarstedt, M. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*; Sage Publications: Thousand Oaks, CA, USA, 2016.

89. Ringle, C.M.; Wende, S.; Becker, J.M. SmartPLS 3. Boenningstedt: SmartPLS GmbH. *J. Serv. Sci. Manag.* **2015**, *10*.

90. Tavakol, M.; Dennick, R. Making sense of Cronbach's alpha. *Int. J. Med. Educ.* **2011**, *2*, 53.

91. Kalkbrenner, M.T. Alpha, Omega, and H Internal Consistency Reliability Estimates: Reviewing These Options and When to Use Them. *Couns. Outcome Res. Eval.* **2021**. https://doi.org/10.1080/21501378.2021.1940118.

92. Ahmad, S.; Zulkurnain, N.N.A.; Khairushalimi, F.I. Assessing the Validity and Reliability of a Measurement Model in Structural Equation Modeling (SEM). *Br. J. Math. Comput. Sci.* **2016**, *15*, 1–8. https://doi.org/10.9734/bjmcs/2016/25183.

93. Eom, S.B.; Ashill, N. The Determinants of Students' Perceived Learning Outcomes and Satisfaction in University Online Education: An Update. *Decis. Sci. J. Innov. Educ.* **2016**, *14*, 185–215. https://doi.org/10.1111/dsji.12097.

94. Cronbach, L.J. Coefficient alpha and the internal structure of tests. *Psychometrika* **1951**, *16*, 297–334. https://doi.org/10.1007/bf02310555.

95. Rifon, N.J.; LaRose, R.; Choi, S.M. Your Privacy Is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures. *J. Consum. Aff.* **2005**, *39*, 339–362. https://doi.org/10.1111/j.1745-6606.2005.00018.x.

96. Boss, S.R.; Bentley University; Galletta, D.; Lowry, P.; Moody, G.D.; Polak, P.; University of Pittsburgh; City University of Hong Kong; Florida International University What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. *MIS Q.* **2015**, *39*, 837–864. https://doi.org/10.25300/misq/2015/39.4.5.

97. Yi, M.Y.; Jackson, J.D.; Park, J.S.; Probst, J.C. Understanding information technology acceptance by individual professionals: Toward an integrative view. *Inf. Manag.* **2006**, *43*, 350–363. https://doi.org/10.1016/j.im.2005.08.006.

98. Clegg, C.W.; Unsworth, K.; Epitropaki, O.; Parker, G. Implicating trust in the innovation process†. *J. Occup. Organ. Psychol.* **2002**, *75*, 409–422. https://doi.org/10.1348/096317902321119574.

99. Adhikari, K.; Panda, R.K. Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks. *J. Glob. Mark.* **2018**, *31*, 96–110. https://doi.org/10.1080/08911762.2017.1412552.

100. Pavlou, P.A. Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *Int. J. Electron. Commer.* **2003**, *7*, 101–134. https://doi.org/10.1080/10864415.2003.11044275.

101. Li, X.; Hess, T.J.; Valacich, J.S. Why do we trust new technology? A study of initial trust formation with organizational information systems. *J. Strat. Inf. Syst.* **2008**, *17*, 39–71. https://doi.org/10.1016/j.jsis.2008.01.001.

102. Mohamed, N.; Ahmad, I.H. Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Comput. Hum. Behav.* **2012**, *28*, 2366–2375. https://doi.org/10.1016/j.chb.2012.07.008.

103. Liang, H.; Xue, Y. Understanding security behaviors in personal computer usage: A threat avoidance perspective. *J. Assoc. Inf. Syst.* **2010**, *11*, 394–413, 463. https://doi.org/10.17705/1jais.00232.

104. Solove, D.J.; Citron, D.K. Risk and anxiety: A theory of data-breach harms. *Tex. L. Rev.* **2017**, *96*, 737.

105. Tu, Z.; Yuan, Y.; Archer, N. Understanding user behaviour in coping with security threats of mobile device loss and theft. *Int. J. Mob. Commun.* **2014**, *12*, 603. https://doi.org/10.1504/ijmc.2014.064915.

106. Tassabehji, R.; Kamala, M.A. Improving E-Banking Security with Biometrics: Modelling User Attitudes and Acceptance. In Proceedings of the 2009 3rd International Conference on New Technologies, Mobility and Security, Cairo, Egypt, 20–23 December 2009; pp. 1–6. https://doi.org/10.1109/ntms.2009.5384806.

107. Workman, M.; Bommer, W.H.; Straub, D. Security lapses and the omission of information security measures: A threat control model and empirical test. *Comput. Hum. Behav.* **2008**, *24*, 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005.

108. Zhang, X.; Han, X.; Dang, Y.; Meng, F.; Guo, X.; Lin, J. User acceptance of mobile health services from users' perspectives: The role of self-efficacy and response-efficacy in technology acceptance. *Inform. Health Soc. Care* **2016**, *42*, 194–206. https://doi.org/10.1080/17538157.2016.1200053.

109. Grimmelmann, J. Some skepticism about search neutrality. In *The Next Digital Decade: Essays on the Future of the Internet*; TechFreedom: Washington, DC, USA, 2010; pp. 435–459.

110. Davis, F.D. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q.* **1989**, *13*, 319–340.