

Does Privacy Awareness Matter? A Study of Voice Assistant Related Privacy and Security Concerns

Zafrin Malek Mithila¹[0009-0008-0837-5372] and Truth Lumor²[0000-0002-2152-5231]

¹ Cranfield University, Shrivenham, UK. zmmithila@outlook.com

² Cranfield University, Shrivenham, UK. truth.lumor@cranfield.ac.uk

Abstract. Internet of Things (IoT) and Voice Assistant (VA) devices and services have become part of our lives. Probably the COVID-19 pandemic accelerated the rate of adoption and diffusion of these technologies as individuals had to adjust their lives and create new ways of working. However, despite their enormous utility, e.g., in entertainment, home security, care homes, supply chain, and logistics, they pose security and privacy threats. Thus, users are expected to exhibit behaviours that protect their privacy and ensure their security. However, there exists a privacy paradox, i.e., users' security and privacy concerns do not reflect in their use and privacy protection behaviours. To contribute to this discussion, this research set out to investigate the antecedents of *concerns*. Understanding what creates concerns in users may provide a clue to the privacy paradox. Drawing on the literature, a parsimonious model that relates knowledge, awareness, attitude and concerns was tested using data from 123 participants. The results show that indeed knowledge leads to awareness but neither awareness nor knowledge engenders concerns in users. Attitude on the other hand is directly related to concerns. These results highlight the complexity and nebulous nature of the virtual world and call for a relook at knowledge and awareness creation programmes, and the extension of policies and device-level security to augment the behaviours of users. Other implications for theory, policy, and practice are discussed.

Keywords: Concerns, Awareness, Knowledge, Attitude, Privacy Paradox, Internet of Things (IoT), Voice Assistant (VA).

1 Introduction

The Internet of Things (IoT) is an age that has emerged in recent decades as a result of the quick advancement of technology. Voice-controlled technologies have become quite popular, and artificial intelligence assistants like Alexa, Google Assistant, and Siri have become indispensable in our daily lives [1]. According to a poll by Gartner Research Circle, in 2021, 41% of organizations were already using virtual assistants or were expecting to use them by 2022 [2]. Global exports of smart speakers are expected to reach 200 million units by 2022 or 2023, according to Statista [3].

Although these voice-assistant (VA) devices have utility in several areas and are convenient to use, they also raise serious privacy and security issues. IoT and VA devices capture an immense amount of personal information about individuals and are vulnerable to manipulation by malicious actors for a variety of harmful intents as the devices become more integrated into our homes and everyday lives [4]. These vulnerabilities endanger the security and privacy of users and expose them to a variety of attacks ranging from monitoring users to spreading malware [5], [6]. Although such gadgets have certain regulations and standards built in, including GDPR and HIPPA, for gathering personal information, health and financial facts, they are insufficient and occasionally difficult to implement effectively [7]–[9].

Further, the fact that some users may have inadequate knowledge and awareness of the complex security and privacy risks posed by these devices and services creates a breeding ground for prospective cyber threats. As a result, it is critical to inform users of the nature of these threats and provide them with the information necessary for safeguarding themselves in a virtual world where security and privacy risks, their likelihood and impact can be nebulous.

Furthermore, research shows there exists privacy paradox which suggests that users do not behave in ways that protect their security and privacy even if they have privacy and security concerns [10], [11]. One way to approach unravelling this paradox is to understand what engender privacy and security concerns. In the literature, there are findings that link knowledge, awareness, and attitude to concerns and behavioural intent in the physical security context [12], [13] or cyber/information systems security and privacy in organizational contexts [14] [15]. Drawing on the literature, this research seeks to answer the research question: *What creates privacy and security concerns in users regarding IoT and VA devices and services?*

We theoretically developed a research model that related knowledge, awareness, attitude, and concerns and evaluated the model using cross-sectional data from 123 participants. The results show that, although knowledge leads to awareness, knowledge and awareness do not lead to concerns even for people who have positive attitude towards protecting their privacy and security. However, attitude directly influence concerns. Our findings are in line with the privacy paradox [10], [11] and other findings [16]. However, it brings to the fore the nebulous nature of the virtual world and the seemingly inability of users to adequately identify and assess risks, and choose behaviours that protect their security and privacy. It also highlights the need to extend policies to cover user information that are collected without the user's knowledge, e.g., information collected when voice assistant devices eavesdrop on conversations. That falls outside the provision of consent which is required by several policies, e.g. GDPR. Further, it highlights the need to relook at public security and privacy knowledge and awareness creation programmes. These programmes should not only concentrate on passing on information but should find ways to embed users in the virtual world in ways that make security and privacy threats more concrete and visible to them in order to influence their privacy protection behaviours. We discuss other implications for policy, practice, and research.

The rest of the paper is structured as follows. The literature review, methodology, data analysis, and discussions, are presented in section 2, section 3, section 4, and section 5 respectively.

2 Literature Review

2.1 IoT and Voice-Controlled Devices

The Internet of Things (IoT) makes life easier by connecting many gadgets, people, and the services and applications that support them. Although it improves the user's experience, the security of IoT devices may be compromised by a single vulnerability. IoT devices in a smart home can be vulnerable to both internal and external threats; malicious attackers can steal private information stored on the devices, monitor the user's life, or if necessary, use the user's personal information unauthorizedly. This information can be accessed using techniques of social engineering or by intercepting primary data collected through IoT sensors [17].

Things or devices that are connected to the Internet using ubiquitous technologies can be accessed from any location, which refers to the Internet of Things (IoT) [18]. Machine-to-machine (M2M) communication is only one of the many services it provides, but it extends much beyond that. An object must be able to communicate across a personal or public network in order to be considered IoT-enabled. It expands the concept of smart technology to encompass devices that can be controlled from any location at any time using the Internet. Personal health care, surveillance systems, home automation, and connected vehicles are just a few of the many domains where IoT devices share and exchange valuable data.

However, voice assistant devices are software programs that can recognize and respond to human speech using artificial voices [1]. It is activated by hearing a certain word or phrase [19]. After hearing that term, the device records the user's speech and transmits it to the server, where it is processed and interpreted as an instruction. In response, the server will provide the voice-controlled device with the necessary information to complete the specified activities with various connected devices and applications [1]. Voice-controlled devices have been in the market for more than a decade and in terms of essential functions, all are similar. Being internet-enabled technologies, it aids users in a wide range of tasks, from scheduling alarms and playing music to connecting with others [20], [21]. In addition to its uses for conversation and companionship, it may also be utilized as a tool for online shopping, studying, and controlling other smart applications and gadgets[21].

2.2 Security and Privacy Concerns

Several academic researchers have raised concerns about the security, privacy, and general dependability of VA devices. Such concerns may take many different forms, from attackers taking advantages of device flaws to the possibility of listening in on user conversations with these always-on gadgets[17]. A rising number of individuals are

embracing smart assistants, such as Alexa or Google Assistant, but recent occurrences are making such doubt if they can completely trust these digital gadgets with their personal information [4]. In the past, VA devices have been blamed for sending private conversations or misinterpreting wake phrases [4]. A notable weakness noted in the literature is the infrequent inability of some VA devices to correctly interpret wake phrases, opening a door for the malicious actors [4].

Emerging threats like Voice Squatting attacks (VSA) and Voice Masquerading attacks (VMA) along with the incidents like the Mirai botnet attack, highlight the dynamic nature of VA and IoT device vulnerabilities and how attackers exploit using speech or the device itself to activate adverse skills [22], [23]. Moreover, the vulnerabilities of VA devices have been highlighted by recent academic research as well. For example, acoustic attacks show how easily malicious actors may take control of these devices by using the Near-Ultrasound Inaudible Trojan (NUIT) and other related vulnerabilities [22], [24], [25]. In regard to NUIT, it just needs a few seconds of elevated noise and an active voice assistant to exploit the system. Several earlier incidents, including SurfingAttack, DolpinAttack, LipRead and SlickLogin also targeted smart home assistants and exploit vulnerabilities in these systems [26].

On the other hand, incidents of unintentional device activations appear as sharp reminders of the necessity of effective security measures. Third-party voice application development also presents a new vulnerability because inadequate security verification procedures are still in place. The story of a young child accidentally activating an Echo Dot to a Super Bowl commercial stealing a Google Home device, highlight the possible repercussions when VA devices are misused [4], [26].

In all IoT applications, including VA technology, security and privacy have always been a major concern. Despite that, domestic IoT devices are frequently utilized. According to certain studies, the risk associated with the VA or IoT devices differs depending on the user's demography [17], [27]. Some others cited a lack of understanding among users as to how to use these devices safely [28]–[31]. Also, some cited as an attacker may get access to the system by exploiting the device's failure to understand the wake word [1], [23]. Some studies have discovered a discrepancy between user's views regarding privacy and their subsequent actions, in which consumers consider the potential risks of sharing personal data against the potential advantages of using those devices [28]. Security breaches arise when privacy settings are not updated, and patches are not discovered. The review of related literature shows that the majority of researchers agree that user awareness is important as consumers awareness related to IoT and VA devices are lacking.

2.3 Advancements in Policy and Research

A few studies have focused on the crucial intersection between security research and policies as they relate to voice assistant devices, especially in the context of IoT technology in general. Many emphasizes the importance of the European General Data Protection Regulation (GDPR) in establishing online user's right to data protection and privacy [9], [32], [33]. It clarifies how GDPR might be used to limit inappropriate gathering and storing of data techniques, particularly in the context of speech recognition

technology, where data privacy issues are of utmost importance. As an option to stop data gathering and processing practices that can contradict GDPR laws, Article 66 of the GDPR is recommended [32]. Additionally, the discussion goes into the purposeful use of the inaccurate language in the privacy policies, which creates a discrepancy between user expectations and legal complexities, mandating a clearer and user-centric approach to policy formation [7]

Furthermore, Liao [7] highlights the efforts of VA platform providers to assure data safety and privacy, particularly for skill creators. Despite the presence of policies, the analysis finds significant shortcomings in their efficient application, notably with regard to the gathering of health data and the identification of sensitive information. It highlights that the need for more in-depth and comprehensive security policies is obvious, requiring enhanced knowledge, clearer compliance criteria, as well as more robust laws and regulations to protect user privacy rights.

2.4 Development of Research Model

In this subsection, we propose a research model of hypothesized relationships among user awareness, knowledge, concerns and attitudes relating to the security and privacy of the IoT or VA devices. **Fig. 1** represents the links among the various constructs as described below.

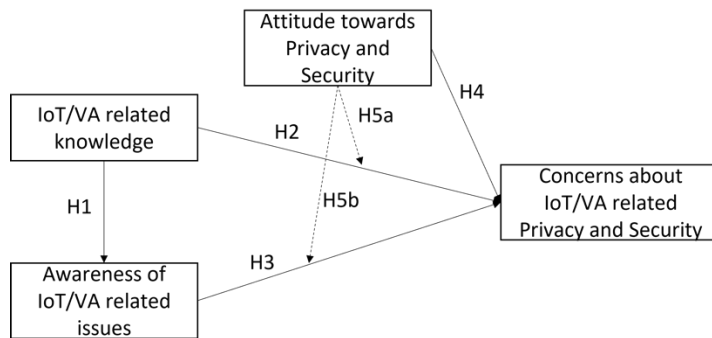


Fig. 1. Hypothesized model of IoT/VA related privacy and security

Knowledge and Awareness. Knowledge and awareness are sometimes used interchangeably [12], [34], [35]. Here, like in other studies e.g., [13], [35], we separate these two constructs to gain a better understanding of their influence on user security and privacy concerns. Knowledge is seen as an emergent concept from humans engaging in the process of knowing[34]. Knowledge can be experiential, skill-related, and a claim [34]. It can also be explicit, e.g., knowledge communicated in this paper, or tacit, e.g., the craft of writing this paper [34]. Knowledge is what comes to be when a person acquires contextual information about something, skills to do something or experience of something whose existence the one knowing believes or can imagine (or construct). Knowledge, thus can be gained from education [36], [37] and training programmes

[37], [38], and experience within a particular context [12]. For instance, when users actively search for and read security policies governing their IoT devices and services, they gain knowledge of that context.

Awareness on the other hand is the internalization of what is known in order to appraise its implications. It follows from the acquisition of knowledge [12]. For instance, Information Security Awareness is conceptualized to include a user's state of consciousness, state of mind, and knowledge [39], [40] and have the ability to project the impact of information security elements now and in the future [40].

Research has linked education [36], [37], [41] and knowledge [38], [39] to awareness. In line with the literature, we argue for a similar relationship in the context of VA devices and services. When users gain more knowledge about IoT or VA devices and services and associated privacy and security issues, their awareness of such issues will increase. Thus, we suggest the following hypothesis:

H1: Users' knowledge of IoT or VA devices and related security and privacy issues will be positively related to their awareness of the same.

Knowledge and Concern. Users' privacy and security concerns have received attention in the literature [40], [42]–[44]. Privacy and security concerns arise when a user feels their information is vulnerable and they lack control over their information [43], [44]. Concern can occur at different levels and in different contexts [42]. For instance, a user can be concern about the privacy and security of their information that they share with their colleagues on the on hand, and information that they share (willingly or otherwise) whilst they transact online, e.g., procuring products or services virtually [44]. The more users have knowledge of the use context, e.g., the extent to which their information can be shared, stolen, used to impersonate, the more concerned they will be. For instance, Dinev and Hart [44] suggest that perceived vulnerabilities and perceived ability to control ones information respectively have strong and moderate influence on ones perceived privacy concern. Users' concerns about IoT or VA device security and privacy develop as their knowledge of those devices and associated security and privacy issues expands. Hence, we suggest the following hypothesis:

H2: Users' concerns about IoT or VA devices and their associated privacy and security issues will increase as their knowledge of the devices and issues increase.

Awareness and Concern. Awareness provides an intricate and deep-seated appraisal of what we know and its implication in context [39], [40]. It relates to the feeling of responsibility or at least the urge to guard against the implications of what one knows [45]. For instance, having a good appreciation of the possible implications of identity theft, or compromises to personal security or privacy by making one's location data available, is likely to arouse concern in a user. Research has shown that users may be aware or concerned but may not have the capability or, in some cases, the willingness to pursuer approved behaviours [16]. This is also captured in the privacy paradox [10], [11]. However, in this paper, we are interested in the extent to which awareness arouses concerns in the user. As users grow in their awareness of IoT or VA devices and related privacy issues, they will tend to develop concerns. They will become more vigilant of

data collection and use as well as concerned about giving out personal information. Thus, suggest the following hypothesis:

H3: A user's IoT or VA device related security and privacy concerns are influenced by his/her security and privacy awareness.

The Effect of Attitude. Attitude is “a psychological tendency that is expressed by evaluating a particular entity with some degree of favor or disfavor” [46, p. 1]. It reflects the degree to which an individual values a behaviour [47], [48]. Broadly, attitudes are formed around *an entity* or “attitude objects” [48] which are the focus of the individual's attitude. Examples of attitude objects include privacy or security [49], [50], IT adoption and use [43], [51], and compliance [47], [52]. The attitude of an individual towards personal information security and privacy will thus mean the extent to which the individual values his/her privacy and security.

Perceptions of IoT or VA security and privacy are greatly influenced by a user's attitude. Based on several factors including information, privacy expectations, benefit preferences, and general concerns, a user's value perception of IoT or VA device privacy differs which may influence his/her level of concern. We thus propose the following hypotheses:

H4: A user's attitude towards IoT or VA related security and privacy will influence the users concern

H5a: A user's attitude towards IoT related security and privacy will moderate the relationship between the user's knowledge and concern about IoT or VA related privacy and security issues.

H5b: A user's attitude towards IoT related security and privacy will moderate the relationship between the user's awareness of and concern about IoT or VA related privacy and security issues.

3 Research Method

3.1 Construct Measurement and Questionnaire Development

A questionnaire was developed and used to collect the data. In this study, the constructs identified from the literature review are operationalized using measures from the literature as summarized in the table below. Knowledge was measured using a 5-item scale adapted from Khando et al. [37] and Haeussinger and Kranz [39]. Following Bulgurcu et al. [47] and Dinev et al. [44], we split awareness into two, namely general awareness and situational-specific awareness. The two constructs are different dimensions of awareness. We adapted the two to multidimensionally measure user awareness of IoT-related privacy and security awareness. Concern for IoT-related security and privacy was measured by adapting the concern construct from Zhang et al. [42] and Sheng et al. [43]. Attitude towards personal privacy and security was adapted from Bulgurcu et al. [47]. The items were measured with a like-it scale from 1 (totally disagree) to 5 (strongly agree). Also, age and formal education were included as control variables.

Age and formal education are likely to influence the degree of knowledge, awareness and concern that how has towards IoT-related privacy and security [37], [41], [53]. The items were then used to develop a questionnaire using the Qualtrics platform.

Table 1. Constructs

Construct	Source
Knowledge of IoT	Khando et al.[37] and Haeussinger and Kranz [39].
Attitudes Toward Security and Privacy	Bulgurcu et al. [47]
VA Awareness (General)	Bulgurcu et al. [47], Dinev et al. [44]
VA Awareness (User Specific)	Bulgurcu et al. [47]
Concern for security and privacy	Zhang et al. [42]& Sheng et al. [43]

3.2 Data Collection

The data was collected using an online questionnaire delivered through Qualtrics. Research participants were sought by sending emails to the cohort of the first author and other students within her networks. Participants were also invited from LinkedIn and other platforms. The questionnaire was made available for two months and reminders were sent to research participants via emails, text messages, and instant messages.

The first author sought ethical clearance and as a consequence asked the research participants for their informed consent and assured them that they were under no obligation to complete the survey. In other words, the survey was free and respondents were given no incentives.

A total of 173 replies were recorded, however, only 123 were fully completed questionnaires. All questionnaires that were not fully completed, thus having missing data, were excluded from the analysis.

4 Data Analysis and Results

Please note that the first paragraph of a section or subsection is not indented. The first paragraph that follows a table, figure, equation etc. does not have an indent, either. Subsequent paragraphs, however, are indented.

4.1 Preliminary Analyses

Research Participants. Most of our research participants ($N = 103$, ~83.60%), are within the age bracket 25-44 years old. There were 37, 70, and 10 research participants whose highest formal education was Bachelor, Master, and PhD degrees, respectively. Taken together, over 95% of the participants had an adequate level of education to read

and understand security and privacy policies and guidelines. These two variables, age and formal education, are used as control variables in the regression models.

Theoretical Constructs. We used Cronbach alpha to verify the loading of the scale items on their various theoretically specified factors (i.e., constructs) [54]. Cronbach alpha can be used as an indicator of internal consistency, i.e., the extent to which theoretically specified items measure the same construct [55]. Cronbach alpha (α) values greater than .7, .8, and .9 are acceptable, good, and excellent respectively [54]. However, alpha values > 0.90 may indicate redundancies [55]. Results from our internal consistency analysis yielded Cronbach alpha (α) greater than .8 for all constructs. The Awareness construct is a composite scale from the combination of general awareness (GenAware), and specific awareness (SpecAware) which yields $\alpha = .82$. We summarize the results in **Table 2**.

Table 2. Cronbach Alpha of Constructs

Construct	raw_alpha	std.alpha	G6(smc)	average_r	S/N	ase	mean	sd	median_r
Knowledge	0.81	0.82	0.81	0.48	4.60	0.027	4.00	0.71	0.50
GenAware	0.84	0.84	0.83	0.52	5.40	0.022	3.60	0.80	0.51
SpecAware	0.90	0.90	0.90	0.61	9.30	0.014	3.30	0.92	0.62
Concerns	0.87	0.87	0.89	0.52	6.60	0.019	4.10	0.70	0.53
Attitude	0.84	0.84	0.81	0.57	5.30	0.023	4.30	0.65	0.57
Awareness*	0.82	0.82	0.70	0.70	4.60	0.03	3.40	0.79	0.70

* A combined scale of GenAware and SpecAware

Descriptive Statistics. As illustrated in **Table 3**, we retained 123 fully completed questionnaires ($N = 123$). Thus, there are no null values or na (not applicable) values in our data. The table shows measures of central tendency (e.g., mean and median), measures of dispersion (e.g., std.dev and var), and indications of normality (skew and kurtosis).

Table 3. Descriptive Statistics

	Knowledge	Concerns	Attitude	Awareness
nbr.val	123.0000	123.0000	123.0000	123.0000
nbr.null	0.0000	0.0000	0.0000	0.0000
nbr.na	0.0000	0.0000	0.0000	0.0000
min	2.0000	2.0000	2.0000	1.0000
max	5.0000	5.0000	5.0000	5.0000
range	3.0000	3.0000	3.0000	4.0000
median	4.0000	4.1667	4.2500	3.5333
mean	3.9561	4.0637	4.2805	3.4280
SE.mean	0.0638	0.0633	0.0582	0.0714
CI.mean.0.95	0.1262	0.1254	0.1152	0.1414
var	0.5000	0.4934	0.4166	0.6271
std.dev	0.7071	0.7024	0.6454	0.7919
coef.var	0.1787	0.1729	0.1508	0.2310
Skew	-0.4800	-0.6900	-0.9400	-0.3600
Kurtosis	0.0800	0.2100	0.8300	0.100

4.2 Hypotheses Testing

We turn our attention to testing our hypotheses. We do so through building and testing 7 models as illustrated in Table 4. In Model1 (M1), we regressed the control variables, i.e., age and formal education, and knowledge on awareness. The results show that although the control variables do not influence awareness, knowledge does ($R^2 = .138$, $F(3, 119) = 6.341$, $p < .000$). Conversely, neither Awareness in Module2 ($R^2 = .039$, $F(3, 119) = 1.6$, $p = .193$) nor Knowledge in Module3 ($R^2 = .026$, $F(3, 119) = 6.341$, $p = .375$) influence a user's IoT security and privacy concerns. Results from Module4 ($R^2 = 0.083$, $F(3, 119) = 3.606$, $p < 0.05$) show that Attitude influences a user's IoT security and privacy concerns. However, Attitude does not moderate the relationship between Awareness and Concern, nor does it the relationship between Knowledge and Concern as shown in Model5 ($R^2 = .11$, $F(3, 119) = 2.892$, $p = 0.017$) and Module6 ($R^2 = .089$, $F(5, 117) = 2.292$, $p < 0.05$), respectively. We also examined the possible mediated relationship between Knowledge and Concern. Contrary to our hypothesis, such a relationship does not exist in the data ($R^2 = .11$, $F(6, 116) = 2.416$, $p < 0.05$). Finally, we regressed knowledge ($\beta = 0.041$, $p > 0.05$), awareness ($\beta = 0.091$, $p > 0.05$), and attitude ($\beta = 0.263$, $p < 0.05$), on concerns and found that only attitude influenced concern ($R^2 = .098$, $F(5, 117) = 2.550$, $p < 0.05$).

Table 4. Results of Regression Analysis

Variables (sig. code)	M1 (Aware)	M2 (Con)	M3 (Con)	M4 (Con)	M5 (Con)	M6 (Con)	M7 (Con)	M8 (con)
Intercept	2.461 ***	3.170 ***	3.339 ***	2.507 ***	4.657 *	2.194	4.535 *	2.059 **
Age	-0.098	0.129	0.116	0.114	0.108	0.114	0.106	0.122
Formal Edu.	-0.117	0.010	-0.007	-0.006	0.000	-0.009	-0.002	0.002
Knowledge	0.394 ***	-	0.092	-	-	0.086	0.040	0.041
Awareness	-	0.132	-	-	-0.629	-	-0.630	0.091
Attitude	-	-	-	0.280 **	-0.282	0.285	-0.276	0.263 **
Awareness*Attitude	-	-	-	-	0.164	-	0.162	-
Knowledge*Attitude	-	-	-	-	-	-0.003	-	-
R-squared	0.138	0.039	0.026	0.083	0.110	0.089	0.111	0.098
Adj R-squared	0.116	0.015	0.001	0.060	0.072	0.050	0.065	0.059
F-Statistic	6.341 ***	1.600	1.046	3.606 *	2.892 *	2.292.	2.416.	2.550. •

Significance codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

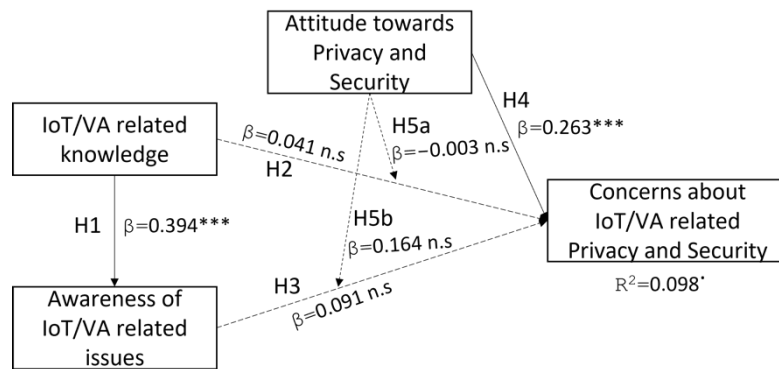


Fig. 2. Verified model of IoT/VA related privacy and security

5 Discussion

IoT and VA devices and services have become an integral part of our lives. Despite their several benefits to users [1], [4] they also pose security and privacy concerns [5], [6]. In this research we investigated the relationship between user knowledge of, awareness of, attitude towards, and concerns about IoT/VA devices and their related privacy and security issues. Drawing on a cross-sectional survey data from 123 research participants, we tested hypothesized relationships using regression analysis. The results of our analysis show that user knowledge indeed influences user awareness of IoT/VA devices and related issues. Specifically, a unit increase in user knowledge results in approximately 0.4 unit increase in user awareness. However, neither awareness nor knowledge directly influence user concerns. The results also show that although a user's attitude is positively related to his/her concerns, it does not moderate the relationship between knowledge and concern or the relationship between awareness and concerns. These findings have implications for theory and practice which we discuss next.

5.1 Implications for Theory

Firstly, the link between knowledge and awareness is consistent with the literature [38], [39] and begs a comprehensive design to capture the complex and multidimensionality of knowledge [37], [39] and awareness [28], [44], [47]. For instance, our analysis showed that knowledge, as we measured it, has different levels of effect on general and specific awareness (not reported in Table 2). Measurements with single-item scales and binary questions, e.g., in [41], miss the complexity of the constructs.

Secondly, the unsupported hypothesized links between concerns and its antecedents (knowledge and awareness) show that the actual links are more complex and nebulous than what is captured in our parsimonious model [44]. This begs further investigation into these relationships and a relook at knowledge enhancing and awareness creation programmes [38]. If enhancing knowledge and awareness does not influence concern, then, do awareness creation programmes in organizations and society (to individuals) matter? We argue they do but under certain conditions of mediators and moderators that our model did not capture. This complexity might be influencing what is called the security paradox [10], [11]. The security paradox shows that even when individuals have and express their privacy and security concerns, that is not reflected in their security protection behaviours [10], [11]. One will assume that when users have security concerns, they should behave in ways that protect their security. However, the security paradox suggests that they do not, just as our results show that they do not become concerned even when they have knowledge and are aware of the privacy and security issues relating to IoT devices and services. Results from Barth et al. [16] also reflect these findings. Barth et al. [16] found that highly educated users who have the technical capacity to understand and be aware of privacy and security issues and have financial resources to afford secure options indulge in behaviours that are detrimental to their privacy and security.

Thirdly, the results highlight the nebulous nature of the virtual world and the risk of literally transferring interventions and mechanisms from the physical to the virtual world. There are research results that show that in the physical world, knowledge and awareness lead to expected behaviours [12], [13]. Sas et al. [13] show that training employees on physical security can improve the understanding, awareness and security-protecting behaviour of employees, and Safari et al. [12] found that environmental knowledge and awareness translate into managers' green behaviour. These results are likely because the objects and impact of physical security are more apparent than the objects and impact of security in the virtual world. In other words, employees or users are more likely to apprehend the objects of security and appreciate the losses, costs, and impacts of security breaches in the physical world than they are likely to do in the virtual world. Hwang et al. [14] show that the extent to which employees can observe security processes, activities, and incidents in an organization influences their awareness and subsequently their security compliant behavioural intentions.

Besides, it is worth noting that most of these studies are embedded within social contexts making their results subject to influences within such social contexts in ways that are difficult to replicate in individual-level studies like this one. Factors such as managerial support and participation [14], social pressure within organizations [56] security compliance monitoring and evaluation [57], and organizational security culture [15] influence employees' knowledge and awareness of security issues and their subsequent compliance intentions. Thus, future research should look into the design of security and privacy knowledge and awareness creation interventions such that they improve the visibility of security and privacy risks and costs in the virtual world and create the contextual factors that translate knowledge and awareness into concerns and security and privacy protection behaviours.

Fourthly, the findings suggest that the missing links between concerns and its antecedents do not depend on the attitudes of users although users' attitudes directly influence their concerns. This suggests that, in addition to improving knowledge and creating awareness, programmes targeted at improving users privacy and security behaviours should contain interventions towards improving users' attitudes e.g., through social influences [56], [58] and improved visibility and impact of security and privacy breaches [14] in IoT/VA environments.

5.2 Implications for Policy and Practice

Our findings have several implications for policy makers, and IoT/VA device/service providers.

Firstly, findings from our research and others e.g., [16], [45], [10] suggest that most individual users appear incapable of translating their knowledge and awareness of IoT/VA related security and privacy issues into concerns and behaviours that protect their security and privacy. This is irrespective of their attitude, resources, and technical capabilities. Policy makers should thus take further actions to protect users from themselves. Policies including GDPR have requirements for consent and the ability of the user to request that information held about him/her are up-to-date. However, these policies are largely limited to information that are actively offered by users, e.g., by filling

in a form or providing some credentials to receive services. Information that is inactively provided, e.g., information that VA devices pick up by eavesdropping on discussions, are not thoroughly covered by these policies, primarily because of their focus on the active involvement of the user e.g., through the provision of consent and the assumption that users always know these devices are collecting information about them. Since technologies are evolving very fast posing new challenges [59], policy makers will find the findings of this research relevant in informing the review of the premise and assumptions of privacy and security policies to protect individual users.

Secondly, device and service providers should consider improving the security and privacy features of these devices and services to augment for the self-destructive security and privacy behaviours of users, especially, individual users [10], [16]. This can be done by, for example, improving the security features that prevent information theft by third parties, and providing notifications to remind users when their conversations that are not targeted at the devices can be heard.

Thirdly, policymakers, social intervention organizations, and device providers should augment the visibility of security and privacy issues by making information collected over IoT/VA devices auditable. By “auditable”, we mean the ability of users to request not only for the “up-to-dateness” of their information, but also to know third parties that have and use their information, and the use to which their information has been put to over a period of time.

Fourthly, public education and awareness creation organizations should provide an “immersive” environment that simulate what goes on in the virtual environment to increase the visibility of privacy and policy concerns and improve user’s ability to value the impact of their privacy behaviours. Some means by which this can be done is through gamification and simulations [45], [60]–[62]. Such education and awareness creation interventions should incorporate social complexities (e.g., social influences, and rippling effect of one user’s security and privacy decisions on the security and privacy of another) to enhance users’ evaluation of their actions. Such comprehensive design of education and awareness programmes is more likely to produce different dimensions of knowledge and awareness, shape users’ attitudes, concerns, and behaviours.

6 Limitations and Future Research

Our research has some notable limitations. Our research draws on a cross-sectional design to study a phenomenon that lends itself more to longitudinal design [63]. For instance, our research could have yielded a different result if we could control the research participants and offer interventions that influence the various constructs were studied over time. We call on other researchers to consider longitudinal research design to study the path from knowledge creation to security and privacy behaviours of users.

Further, our research was limited by the time the first author had to collect data for her research, placing limitations on the number of respondents we could attract whilst maintaining voluntary and non-incentivized participation. Although the descriptive statistics looks good, it would have been more interesting to have more diversity e.g., in

the age, and formal education of the participants. Barth et al. [16] found that even those who are highly educated, have technical competencies, are financially sound do exhibit the security paradox [10]. This is comparable to our findings. What will be particularly interesting is research that unravels the different trajectory that people with different education, technical competencies, financial status, social status and social influences take towards making security and privacy behaviour decisions. We invite researchers to this discussion, especially, with qualitative tools that can unpack the complexities of security and privacy behaviours at the individual level.

7 Conclusion

With the advancement of 5G and 6G technologies and increasing connectivity, the IoT is developing as a key advancement in information technology. While the number of people using IoT devices has grown significantly, so has the potential for security and privacy breaches. This research investigates the relationship between user knowledge, awareness, attitudes and concerns towards IoT/VA devices and their privacy and security issues. The results highlight the nebulous nature of the virtual world and the seemingly inability of users to channel their knowledge and awareness into creating concerns about the security and privacy issues related to IoT/ VA devices and services. We call on researchers, policymakers, device and service developers, and community/ public knowledge and awareness programme managers to reconsider the roles and capabilities of users and design interventions that augment the deficiencies of users in protecting their privacy and security in the virtual world.

Data Availability Statement

Data supporting this study cannot be made publicly available because participants did not provide consent for their data to be made public.

References

- [1] M. B. Hoy, 'Alexa, Siri, Cortana, and more: an introduction to voice assistants', *Med. Ref. Serv. Q.*, vol. 37, no. 1, pp. 81–88, 2018.
- [2] M. Cain and C. Howard, 'Future of work trends: A gartner trend insight report.', 2021. Accessed: Jan. 20, 2023. [Online]. Available: <https://www.gartner.com/document/code/745430?ref=authbody&refval=>
- [3] F. Laricchia, 'Smart speakers - Statistics & Facts. Statista.', 2022. Accessed: Aug. 15, 2023. [Online]. Available: <https://www.statista.com/topics/4748/smart-speakers/#dossierKeyfigures>
- [4] E. Cho, S. S. Sundar, S. Abdullah, and N. Motalebi, 'Will deleting history make alexa more trustworthy? effects of privacy and content customization on user experience of smart speakers', in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–13.

- [5] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, 'IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices', *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8182–8201, 2019.
- [6] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, 'Security, privacy and trust in Internet of Things: The road ahead', *Comput. Netw.*, vol. 76, pp. 146–164, 2015.
- [7] J. Young, S. Liao, L. Cheng, H. Hu, and H. Deng, '{SkillDetective}: Automated {Policy-Violation} Detection of Voice Assistant Applications in the Wild', in *31st USENIX Security Symposium (USENIX Security 22)*, 2022.
- [8] EDPB, 'Guidelines 02/2021 on virtual voice assistants', European Data Protection Board, Formal Version 2, Jul. 2021. Accessed: Sep. 02, 2023. [Online]. Available: https://edpb.europa.eu/system/files/2021-07/edpb_guidelines_202102_on_vva_v2.0_adopted_en.pdf
- [9] N. Olsen, 'Voice Assistants and Privacy Issues'. Accessed: Sep. 02, 2023. [Online]. Available: <https://www.privacypolicies.com/blog/voice-assistants-privacy-issues/>
- [10] P. A. Norberg, D. R. Horne, and D. A. Horne, 'The privacy paradox: Personal information disclosure intentions versus behaviors', *J. Consum. Aff.*, vol. 41, no. 1, pp. 100–126, 2007.
- [11] D. Wilson and J. S. Valacich, 'Unpacking the privacy paradox: Irrational decision-making within the privacy calculus', 2012.
- [12] A. Safari, R. Salehzadeh, R. Panahi, and S. Abolghasemian, 'Multiple pathways linking environmental knowledge and awareness to employees' green behavior', *Corp. Gov. Int. J. Bus. Soc.*, vol. 18, no. 1, pp. 81–103, 2018.
- [13] M. Sas, G. Reniers, K. Ponnet, and W. Hardyns, 'The impact of training sessions on physical security awareness: Measuring employees' knowledge, attitude and self-reported behaviour', *Saf. Sci.*, vol. 144, p. 105447, 2021.
- [14] I. Hwang, R. Wakefield, S. Kim, and T. Kim, 'Security awareness: The first step in information security compliance behavior', *J. Comput. Inf. Syst.*, vol. 61, no. 4, pp. 345–356, 2021.
- [15] J. D'Arcy and G. Greene, 'Security culture and the employment relationship as drivers of employees' security compliance', *Inf. Manag. Comput. Secur.*, vol. 22, no. 5, pp. 474–489, 2014.
- [16] S. Barth, M. D. de Jong, M. Junger, P. H. Hartel, and J. C. Roppelt, 'Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources', *Telemat. Inform.*, vol. 41, pp. 55–69, 2019.
- [17] M. Park, H. Oh, and K. Lee, 'Security risk measurement for information leakage in IoT-based smart homes from a situational awareness perspective', *Sensors*, vol. 19, no. 9, p. 2148, 2019.
- [18] A. M. French and J. P. Shim, 'The digital revolution: Internet of things, 5G, and beyond', *Commun. Assoc. Inf. Syst.*, vol. 38, no. 1, p. 40, 2016.
- [19] J. Lau, B. Zimmerman, and F. Schaub, 'Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers', *Proc. ACM Hum.-Comput. Interact.*, vol. 2, no. CSCW, pp. 1–31, 2018.

- [20] I. Ghafir *et al.*, ‘Security threats to critical infrastructure: the human factor’, *J. Supercomput.*, vol. 74, pp. 4986–5002, 2018.
- [21] V. Pitardi and H. R. Marriott, ‘Alexa, she’s not human but... Unveiling the drivers of consumers’ trust in voice-based artificial intelligence’, *Psychol. Mark.*, vol. 38, no. 4, pp. 626–642, 2021.
- [22] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu, ‘Dolphinattack: Inaudible voice commands’, in *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*, 2017, pp. 103–117.
- [23] L. A. Wahsheh and I. A. Steffy, ‘Using Voice and Facial Authentication Algorithms as a Cyber Security Tool in Voice Assistant Devices’, in *17th International Conference on Information Technology–New Generations (ITNG 2020)*, Springer, 2020, pp. 59–64.
- [24] G. Chen, ‘Uncovering the unheard: Researchers reveal inaudible remote cyber-attacks on voice assistant devices’, UTSA Today. Accessed: Sep. 06, 2023. [Online]. Available: <https://www.utsa.edu/today/2023/03/story/chen-nuit-research.html>
- [25] M. Szabó, ‘Hear no evil: Ultrasound attacks on voice assistants - How your voice assistant could do the bidding of a hacker without you ever hearing a thing’, Welivesecurity. Accessed: Sep. 03, 2023. [Online]. Available: <https://www.welivesecurity.com/2023/06/07/hear-no-evil-ultrasound-attacks-voice-assistants/>
- [26] M. Martinez and L. Cameron, ‘Voice Technology: As Google Duplex Wows and Scares, a Post-Screen World Emerges with Questions that the Smart Speakers Cannot Answer’, IEEE Computer Society. Accessed: Aug. 02, 2023. [Online]. Available: <https://www.computer.org/publications/tech-news/trends/voice-assistants-technology-smart-speakers>
- [27] S. Wells, ‘Internet of Things Security Using Secondary Monitoring’, PhD Thesis, University of Colorado at Boulder, 2018.
- [28] T. Dinev and Q. Hu, ‘The centrality of awareness in the formation of user behavioral intention toward protective information technologies’, *J. Assoc. Inf. Syst.*, vol. 8, no. 7, p. 23, 2007.
- [29] P. A. Wang, ‘Information security knowledge and behavior: An adapted model of technology acceptance’, in *2010 2nd International Conference on Education Technology and Computer*, IEEE, 2010, pp. V2-364.
- [30] E. G. Smit, G. Van Noort, and H. A. Voorveld, ‘Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe’, *Comput. Hum. Behav.*, vol. 32, pp. 15–22, 2014.
- [31] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, ‘The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved’, *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1606–1616, 2018.
- [32] T. Munk, ‘Does online privacy exist in the GDPR era? The Google voice assistant case’, in *EU Internet Law in the Digital Single Market*, Springer, 2021, pp. 479–507.

- [33] L. H. Acosta and D. Reinhardt, 'A survey on privacy issues and solutions for Voice-controlled Digital Assistants', *Pervasive Mob. Comput.*, vol. 80, p. 101523, 2022.
- [34] E. Bolisani, C. Bratianu, E. Bolisani, and C. Bratianu, 'The elusive definition of knowledge', *Emergent Knowl. Strateg. Strateg. Think. Knowl. Manag.*, pp. 1–22, 2018.
- [35] R. Treveltham, 'Deconstructing and assessing knowledge and awareness in public health research', *Front. Public Health*, vol. 5, p. 194, 2017.
- [36] A. R. Ahlan, M. Lubis, and A. R. Lubis, 'Information security awareness at the knowledge-based institution: its antecedents and measures', *Procedia Comput. Sci.*, vol. 72, pp. 361–373, 2015.
- [37] K. Khando, S. Gao, S. M. Islam, and A. Salman, 'Enhancing employees information security awareness in private and public organisations: A systematic literature review', *Comput. Secur.*, vol. 106, p. 102267, 2021.
- [38] M. M. Al-Daeef, N. Basir, and M. M. Saudi, 'Security awareness training: A review', *Lect. Notes Eng. Comput. Sci.*, 2017.
- [39] F. Haeussinger and J. Kranz, 'Information security awareness: Its antecedents and mediating effects on security compliant behavior', 2013.
- [40] J. Correia and D. Compeau, 'Information privacy awareness (IPA): a review of the use, definition and measurement of IPA', 2017.
- [41] K. L. Piercy, F. Bevington, A. Vaux-Bjerke, S. W. Hilfiker, S. Arayasirikul, and E. Y. Barnett, 'Understanding contemplators' knowledge and awareness of the physical activity guidelines', *J. Phys. Act. Health*, vol. 17, no. 4, pp. 404–411, 2020.
- [42] N. A. Zhang, C. A. Wang, E. Karahanna, and Y. Xu, 'PEER PRIVACY CONCERN: CONCEPTUALIZATION AND MEASUREMENT.', *MIS Q.*, vol. 46, no. 1, 2022.
- [43] H. Sheng, F. F.-H. Nah, and K. Siau, 'An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns', *J. Assoc. Inf. Syst.*, vol. 9, no. 6, p. 1, 2008.
- [44] T. Dinev and P. Hart, 'Internet privacy concerns and their antecedents-measurement validity and a regression model', *Behav. Inf. Technol.*, vol. 23, no. 6, pp. 413–422, 2004.
- [45] M. Zwillling, G. Klien, D. Lesjak, \Lukasz Wiechetek, F. Cetin, and H. N. Basim, 'Cyber security awareness, knowledge and behavior: A comparative study', *J. Comput. Inf. Syst.*, vol. 62, no. 1, pp. 82–97, 2022.
- [46] A. H. Eagly and S. Chaiken, *The psychology of attitudes*. Harcourt brace Jovanovich college publishers, 1993.
- [47] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, 'Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness', *MIS Q.*, pp. 523–548, 2010.
- [48] C. M. Angst and R. Agarwal, 'Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion', *MIS Q.*, pp. 339–370, 2009.

- [49] N. Gerber, P. Gerber, and M. Volkamer, 'Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior', *Comput. Secur.*, vol. 77, pp. 226–261, 2018.
- [50] P. Rajivan and J. Camp, 'Influence of Privacy Attitude and Privacy Cue Framing on Android App {Choices}', in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, 2016.
- [51] C. M. Angst and R. Agarwal, 'Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion', *MIS Q.*, pp. 339–370, 2009.
- [52] A. Al-Omari, A. Deokar, O. El-Gayar, J. Walters, and H. Aleassa, 'Information security policy compliance: An empirical study of ethical ideology', in *2013 46th Hawaii International Conference on System Sciences*, IEEE, 2013, pp. 3018–3027.
- [53] H. A. Kruger, L. Drevin, S. Flowerday, and T. Steyn, 'An assessment of the role of cultural factors in information security awareness', in *2011 Information Security for South Africa*, IEEE, 2011, pp. 1–7.
- [54] J. A. Gliem and R. R. Gliem, 'Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales', *Midwest Research-to-Practice Conference in Adult, Continuing, and Community ...*, 2003.
- [55] M. Tavakol and R. Dennick, 'Making sense of Cronbach's alpha', *Int. J. Med. Educ.*, vol. 2, p. 53, 2011.
- [56] S. S. Kim and Y. J. Kim, 'The effect of compliance knowledge and compliance support systems on information security compliance behavior', *J. Knowl. Manag.*, vol. 21, no. 4, pp. 986–1010, 2017.
- [57] M. Alqahtani and R. Braun, 'Examining the Impact of Technical Controls, Accountability and Monitoring towards Cyber Security Compliance in E-government Organisations', 2021.
- [58] S. Youn, 'Parental influence and teens' attitude toward online privacy protection', *J. Consum. Aff.*, vol. 42, no. 3, pp. 362–388, 2008.
- [59] T. Lumor, M. Pulkkinen, A. Hirvonen, and P. Neittaanmäki, 'Creating the Socio-Technical Context Needed to Derive Benefits from Big Data Initiatives in Healthcare', *Scand. J. Inf. Syst.*, vol. 33, no. 2, p. 1, 2021.
- [60] E. G. B. Gjertsen, E. A. Gjære, M. Bartnes, and W. R. Flores, 'Gamification of Information Security Awareness and Training.', in *ICISSP*, 2017, pp. 59–70.
- [61] S. Scholefield and L. A. Shepherd, 'Gamification techniques for raising cyber security awareness', in *HCI for Cybersecurity, Privacy and Trust: First International Conference, HCI-CPT 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26–31, 2019, Proceedings 21*, Springer, 2019, pp. 191–203.
- [62] K. H. Sharif and S. Y. Ameen, 'A review of security awareness approaches with special emphasis on gamification', in *2020 International Conference on Advanced Science and Engineering (ICOASE)*, IEEE, 2020, pp. 151–156.
- [63] J. Porra, R. Hirschheim, and M. S. Parks, 'The historical research method and information systems research', *J. Assoc. Inf. Syst.*, vol. 15, no. 9, p. 3, 2014.

Appendix

Construct/Variable	Items	Scale
Age	How old are you?	Under 18 18 – 24 years 25 – 34 years 35 – 44 years 45 – 54 years 55 – 64 years 65+ years
Level of Education	What is your level of formal education?	Doctorate (e.g., PhD.) Master's Bachelor's Higher Secondary Junior Secondary
Country of Origin	Which one is your country of origin?	A drop-down list of countries
Knowledge	To what extent do you agree with the following? 1. I am familiar with IoT devices. 2. I interact with voice assistant (VA) devices frequently. 3. I know what voice assistant (VA) devices are. 4. I own or have access to a voice assistant (VA) device (e.g., Alexa, Siri, etc.). 5. I know how voice assistant (VA) devices work.	Strongly Disagree (1) – Strongly Agree (5)
Awareness (General)	To what extent do you agree with the following? 2. Overall, I am aware of the potential privacy and security threats of using voice assistant (VA) devices and their negative consequences. 3. I have sufficient knowledge about the cost of potential security and privacy problems related to the use of voice assistant (VA) devices. 4. I read about potential security and privacy problems associated with using voice assistant (VA) devices. 5. I am aware of the policies regarding the provision and use of voice assistant (VA) devices.	Strongly Disagree (1) – Strongly Agree (5)

6. I seek advice regarding the security and privacy of voice assistant (VA) devices.

Awareness (Specific)	To what extent do you agree with the following?	Strongly Disagree (1) – Strongly Agree (5)
	<ol style="list-style-type: none"> 1. While using voice assistant (VA) devices, I read the security and privacy policies associated with the device. 2. I am aware of how the voice assistant (VA) device records my conversations. 3. I am aware of how the voice assistant (VA) device stores and use my data. 4. I am aware of how long my data is stored and protected. 5. I am aware of how my data can be shared with third-party agencies. 6. I know my responsibilities as stated in the security and privacy policy associated with the voice assistant (VA) device I use or have access to in order to enhance my privacy/security. 	
Attitude	Using the options provided, complete the following statements. To me, paying attention to voice assistant (VA) devices related security and privacy policies and the privacy and security of my personal information is...	<ol style="list-style-type: none"> 1. Very important (5) – Very unimportant (1) 2. Very beneficial (5) - Very unbeneficial (1) 3. Very necessary (5) – very unnecessary (1) 4. Very useful (5) – Very useless (1)
Concern	To what extent do you agree with the following?	Strongly Disagree (1) – Strongly Agree (5)
	<ol style="list-style-type: none"> 1. It bothers me that I provide too much personal information whilst using IoT devices, especially, voice assistant (VA) devices. 2. I am concerned that the voice assistant (VA) service provider has too much personal information about me. 3. I am concerned that my personal information could be used in ways I could not foresee. 4. I am concerned that the voice assistant (VA) service provider can use my personal information for other purposes. 	

5. I am concerned that the voice assistant (VA) service provider can UNINTENTIONALLY expose my personal information to third-party agencies who are NOT in our policy agreement.
 6. I am concerned that the voice assistant (VA) service provider can UNINTENTIONALLY expose my personal information to third-party agencies who are in our policy agreement.
-



DSPACE

<https://dspace.org/>

Does privacy awareness matter? A study of voice assistant-related privacy and security concerns

Mithila, Zafrin Malek; Lumor, Truth

2024-09-18

Springer

https://doi.org/10.1007/978-981-97-3973-8_16

Mithila ZM, Lumor T. (2024) Does privacy awareness matter? A study of voice assistant-related privacy and security concerns. In: AI Applications in Cyber Security and Communication Networks. 9th International Conference on Cyber Security, Privacy in Communication Networks (ICCS 2023), 11-12 December 2023. Lecture Notes in Networks and Systems, Volume 1032, pp. 247-267