International Journal of Management, Knowledge and Learning | ISSN 2232-5697

An Examination of Factors Determining User Privacy Perceptions of Voice-Based Assistants

Biodun Awojobi
University of Dallas, USA
aawojobi1@udallas.edu

Brett J. L. Landry
University of Dallas, USA
blandry@udallas.edu

Purpose: Voice-based assistants have become ubiquitous in our homes and all around us. We interact with voice-based assistants through smartphones, dedicated home devices, or other Internet-connected devices. The proliferation of these devices in our lives makes us question whether the data transmitted through these devices are secure and the role perception of privacy the users of these devices have in the usage of the device. This paper focuses on the user privacy issues specific to two voice-based assistants – Amazon Alexa and Google Assistant using quantitative and qualitative methods. The paper will answer three research questions regarding user privacy perceptions and how a user's technology adoption, smartphone operating system, and demographics influence their perception of privacy.

Study design/methodology/approach: This is a mixed research study where survey data was collected from faculty, staff, and students of a large University in the United States and professional connections globally.

Findings: Privacy perceptions vary based on user age, educational level, gender, smartphone adoption, and technical awareness and expertise.

Originality/value: This study is unique in highlighting the perception of privacy for voice-based assistants and assigning a numerical value based on survey data to the concern. Another feature of the study is its correlation of privacy perception with mobile phone operating systems and the level of technical expertise of voice-based assistant users.

Introduction

The term "Internet of Things" (IoT) was first used by Kevin Ashton in a 1999 presentation and, at that time, was used in the supply chain context (Gubbi et al., 2013). The Internet created a world of interconnectivity between computers and devices across networks without global boundaries. This global reach and ease of use have driven the IoT phenomenon. IoT has grown to include home, medical, mobile, industrial, and enterprise devices that are always powered on and connected to the Internet directly or via an intermediary such as a hub or gateway. For consumers, IoTs include automobiles, cameras, door locks, entertainment systems, garage door openers, home lighting, refrigerators, thermostats, and voice-based assistants (VBAs). Even home robots such as the new Amazon Astro can be considered an IoT. Thus, it is not surprising how the term has metamorphized into something more substantial and is potentially one of the biggest technological disruptors over the next decade, second only to Artificial Intelligence (AI). One of the issues facing information security professionals is IoT's emergence and overall adoption rate, which creates an inherent problem of understanding security gaps (Awojobi & Chang, 2017). According to IoT Analytics, there were 3.8 billion connected IoTs in 2015, 7.0 billion in 2018, and is expected to reach 21.5 billion by 2025 (Lueth, 2018).

IoT insecurity

IoTs are generally easy-to-use and low-powered embedded computing machines that lack necessary security measures. IoT research, especially related to security and privacy, is relevant because of the rapid proliferation of these devices, given their weak security posture. These

Volume 12 (2023) 53–62 | https://www.doi.org/10.53615/2232-5697.12.53-62

devices can work together as an “ecosystem of connected things” (Patel, 2017) and introduce different security challenges along with their connection to the Internet. IoT users do not typically replace their devices every year, and IoTs usually stay connected to both local networks and the Internet until their end of life, creating higher security risks. As with most modern-day digital devices that require software updates to stay current with stability and security vulnerabilities, older devices may not receive software and firmware updates for one of two reasons. First, the device does not have the processor capability and/or the storage capacity required for newer operating systems and features. The second is planned obsolescence, where the manufacturer wants users to purchase more recent versions with new features and capabilities. While these scenarios affect all sorts of technologies and are not limited to IoTs, these devices are more prone to security attacks because users do not regularly perform updates and may not know what operating system version is employed, like on personal computers. This means that securing IoTs requires constant security evaluation cycles.

IoTs are designed to scan the network to find other devices and appliances to control to promote ease of use. According to a 2017 appraisal by Razzaq et Al. (2017), 70 percent of IoTs are very easy to attack. IoTs are plagued with weak access control issues because many have fixed usernames and passwords that cannot be changed or do not require passwords at all. With no way to mitigate a security vulnerability, an attacker might be able to compromise an entire network using the known security flaw of a single IoT on the network.

To properly secure a system, there needs to be an established list of security requirements for IoTs to be resilient to attacks. Resilience to attacks means the system can self-heal and defend against security attacks. The system can accomplish this individually with security baselines set on each IoT or through the interconnectivity facilitated through a gateway device or a smart hub. Creating layers of data access is equally important as ensuring that authentication is required to read sensitive data from the system (Razzaq et al., 2017).

Large numbers of compromised or infected computing devices can be organized into botnets and work together for large-scale distributed denial of service (DDoS) attacks, authentication attacks, and spam platforms. In 2020, 103,699 botnet incidents took place mainly against the financial sector for all types of systems (Poremba, 2020). When IoTs are used as botnets, they are known as thingbots (Atluri, 2017) and are attractive targets due to the weak security posture discussed above.

Perceptions of privacy

The concept of privacy concerning every individual is always evolving. Privacy should be an individual decision, and the choice to share data should be up to the device’s owner. The convenience we get through our exposure to the Internet has far-reaching consequences. As humans, we start out trusting technology and expecting our interactions with technology to be private so long we have a username and password or other forms of authentication. Interestingly, however, it is the information metadata that we are not aware of that can lead to targeted attacks. One of the most referenced scholarly works on privacy, “The Right to Privacy,” by Warren and Brandeis (1890), had a vision, a theoretical and practical perspective of privacy and its issues. Privacy is the right to be withdrawn from the external world and “the right to be left alone.” The validity of the statement is arguable. It can sometimes get misconstrued that privacy is a thing of perception. A piece of private information is what we choose not to share with the public or restricted to a subset of people. Every individual has the right to classify what is private information. Before the age of computers, companies relied on trade secrets stored in vaults and secured storage locations. Now, companies digitize these secrets and keep the information safe using computer security tools and techniques.

Digital privacy applies to all the facets of our lives that interact with technology. For developed countries, this is almost all the sectors of the economy. The amount of data collected and available from agriculture, banking, commerce, communication, healthcare, housing, news, and social media sources is enormous. One can argue that data collecting about human subjects, preferences, and more is the right thing to do. After all, the scientific advancements we have experienced could only have happened because of data collection, analysis, and testing cycles. However, when collected data is in the wrong hands, the possibility of it being used for unethical practices becomes pronounced.

The privacy of digital information is one of the most complicated issues to address as it transcends arenas and can be examined from different standpoints. Digital privacy issues can be addressed from various perspectives: legal, technical, governmental, and ethical. The speed of processing and storage capabilities of computers means that we can store metadata of almost any object, and it can be retrieved in an instant whenever we need it. Around the globe, digital transformation is a major focus for both private and public sector entities.

While IoT is also known as the Internet of Everything (IoE) and includes sub-categories such as Industrial Internet of Things (IIoT) and Internet of Medical Things (IoMT) (Figliola, 2020), this paper will focus specifically on one IoT type, VBAs. VBAs like Amazon Alexa and Google Home are ubiquitous because they are inexpensive, easy to set up, and can perform a wide range of activities.

VBAs introduce a more comprehensive range of privacy issues than traditional personal computers and non-voice-based IoTs. Users can also communicate with their devices using a smartphone application. In both cases, users need to learn what information is being sent to the device manufacturer if the device is stealthily listening to all conversations, the data retention policies, or who else has access to their data. There is a risk of unauthorized personal identifiable information (PII) being sent to unsanctioned locations. Also, when the privacy statements in end-user license agreements (EULA) for VBAs change, users may not be aware of these changes.

The ubiquitous adoption of VBAs like Amazon Alexa and Google Home by consumers and enterprises around the world, either through interaction with these devices physically or via a mobile application, has raised questions about the privacy of VBAs. Primarily because of how close the devices are to the users and the always listening mode of the device. A major concern is that the VBA user does not know who is listening on the other end. One example is thousands of Amazon employees listening to private Alexa voice recordings without the device owner's knowledge or permission (Costello & Guthrie, 2019). Generally, there is little known about users' perceptions and concerns regarding privacy with VBAs despite data privacy breaches, and surprisingly, few studies investigate the impact of privacy breaches with VBAs on users' privacy perceptions.

Data Collection

The creation of information and, ultimately, knowledge starts with data collection. Since VBAs are constantly generating, aggregating, and collecting data, manufacturers have found that the proven path to creating knowledge is collecting the data generated by the devices, even when there is no inherent use of the data. However, because large subsets of data can be mined for information, not collecting or retaining usage and content data equates to a wasted opportunity for developing insights that could become a knowledge base. The volume of data generated and collected by VBAs is both a security and a privacy concern. Data governance is also an issue with consumer VBAs since the device manufacturer determines how long the data can be retained on their system.

Another interesting security component of security and devices connected to the Internet is the transparency of signals sent in and out of the devices. VBAs, for example, are always connected to the Internet to help execute basic voice-activated tasks. Most of the data collected from VBAs should be treated as private and confidential. While a user cannot control when or the type of information the VBA transmits to the manufacturer's servers, they can request every piece of data that the device has collected about the user (Saltzman, 2018).

User preferences

Our personal preferences, habits, driving patterns, when we go to sleep, and when we wake up are all information recorded in databases due to our interactions with other humans and technologies. Typically, these forms of data do not get collected in one transaction or interaction. They get collected through multiple transactions and interactions with several systems. For example, many developed countries operate cashless systems. When a user decides to pay with a credit card, some of the user's information is shared with the vendor. Some vendors will request that customers sign up for a loyalty program, which often requires collecting the customer's phone number and other personal information. All the collected data can be stored in a separate database and referred to as greased data (Moor, 1997). The problem is that this data has been leaked onto the Internet on other private sites in the form of data breaches.

Technical expertise

Users' level of technical expertise may not matter when making privacy-related choices. A technologically savvy and privacy-aware individual may decide to share information on a social media site, even when the consequences of the exposure of such information are known. The blurred lines between privacy awareness and emotional influence on irrational decisions are dynamic. Digital privacy choices are made based on the beliefs and perceptions of what can be shared and what should be kept discreet during communication. "Privacy is commonly identified with solitude, typically associated with temporary physical isolation of an individual from others, but most accurately understood as psychological isolation or separation from a range of phenomena and experiences" (Panichas, 2014). Although the definition provided by Panichas is of privacy and not digital privacy, the interaction of humans with social media modifies the dynamics of this definition of privacy. Social media has become a life brand for some. The Internet age now means that the physical contact and interaction model experienced before the rise of Internet-based social networks has changed. Social media apps and websites have now become a medium of interaction, and participation in social networking has undoubtedly led to the disclosure of personal information on the Internet.

Privacy and government policies

Government policies can address digital privacy issues; however, government policies are not enough. Privacy regulations provide the building blocks to ensure that sufficient data privacy standards are abided-by and that there are consequences for non-compliance, which in most cases are fines and levies to the defaulting organization. Concerning security and privacy, humans remain the weakest link. A government cannot control the choices that individuals make concerning the privacy of their information. A government can, however, develop plans, frameworks, awareness campaigns, and guidelines to help protect the privacy of the citizens. It is left to everyone to embrace a privacy-aware culture.

In 2006, the United States Veteran's Affairs determined that they were compromised, and the information of "over 2 million active-duty and reserve personnel as well as veterans were lost. So, the security of those currently serving in the military may have been compromised, and the bond of trust owed to those who served has been broken" (Savitsky et al., 2009). Citizens trust that their government deploys state-of-the-art technology to prevent security breaches. The chain of trust is broken when such breaches compromise private information. A lack of trust in a system can lead to lower system usage.

A 2019 Pew Research Center survey of 4,272 U.S. adults discovered that "Over 60% of U.S. adults reported that they did not think it was possible to go a day without the government or companies collecting data from them" (Brown, 2019). Eighty-one percent of the U.S. adults who responded to the survey indicated that they believe widespread data collection risks outweigh the benefits. While the sample size does not represent the whole country, it suggests that the perceptions of privacy controls of U.S. adults participating in the survey are unfavorable.

Unlike the United States, which is yet to adopt a national data privacy regulation, the European Union (E.U.) has led consumer privacy efforts globally by enacting the E.U. General Data Privacy Regulation (GDPR). The core aim of the GDPR is "to protect all E.U. citizens from privacy and data breaches in today's data-driven world" (EUGDPR, 2018). Basically, GDPR gives E.U. citizens control over how their data is shared and transmitted, as well as the overall usage of their data. While GDPR does not directly address privacy with VBAs, some components of the regulation do apply. At the core of GDPR is a set of interpretations that include "the right to be forgotten" and "the right to erasure" (GDPR.EU). GDPR was designed to accomplish three goals:

1. Harmonize data privacy laws across Europe.
2. Protect and empower all E.U. citizens' data privacy.
3. Reshape the way organizations across the region approach data privacy.

VBA users can request that their data be deleted; however, the provisions made by GDPR allow VBA manufacturers to process the collected data for training purposes to improve the system (Wachter, 2018).

However, GDPR guidelines do not ensure complete data privacy. Ivanova (2018) described an incident where an E.U. resident's data, which were recordings from the use of Alexa, was sent to another user who had never previously used the VBA product. The recordings sent to the wrong user were already downloaded, and the unintended recipient could listen to all the recordings made from another user's home. Issues like these are a breach of privacy and cause distrust within the user community.

Research questions

This paper explored three research questions to examine user privacy perceptions of voice-based technology adoption.

- Research question one: Do users' privacy perceptions of VBAs vary based on their level of technology adoption?
- Research question two: Do users' privacy perceptions of VBAs vary based on which smartphone operating system they use?
- Research question three: Do users' privacy perceptions of VBAs vary based on user demographics?

The study focused on two VBA brands of VBAs, Amazon Alexa and Google Home because of their established market share and integration capabilities. However, during the survey and the interview, Respondents were allowed to specify "Other" if they did not use either of these two brands and were excluded from the sample.

Methodology

A Qualtrics survey was deployed after receiving university institutional review board (IRB) approval. There were two groups surveyed. The first group was current undergraduate students, graduate students, and faculty members at a large state university. The second group was from one of the author's professional LinkedIn contacts containing approximately 3,500 connections worldwide which expanded the responses to a global audience since the LinkedIn contacts were from all over the world. Participation in the survey was voluntary, and there was no form of coercion, money, or other incentives offered during data collection to the Respondents in either group.

Perceptions of Privacy

Based on the literature review, three factors determine user perception of privacy for VBAs. They are the user's privacy preferences, technology controls, and regulations. User privacy perception is at the intersection of these three factors. User privacy preferences are essential components of identifying the non-technical components of privacy. Technology controls comprise security controls put in place to identify security vulnerabilities and privacy attacks. Technology controls also protect from security and privacy incidents, detect and alert of security and privacy anomalies or incidents, and monitor security and privacy vulnerabilities across VBA. While there are quite a few privacy regulations, like the EU GDPR and the California Privacy Act, that protect consumer privacy, they are not specific to protecting user privacy with VBAs.

With respect to this research, we define the user perception of privacy as the mean calculated value of the three components described above. Our survey collected data regarding the three components defined in a Likert scale. The means of the Likert scale in the survey instrument is from "strongly disagree" to "strongly agree," interpreted as the perception level is low to high. Where low user perception of privacy is represented with a 1 and 5 represents a high perception of user privacy.

Results

Do VBA privacy perceptions vary based on the level of technology adoption?

Research question one examined if users' privacy perceptions of VBAs vary based on their level of technology adoption. Higher perceptions of privacy are related to users' confidence that their privacy is protected. The converse is also true. Lower privacy perceptions are related to less confidence that their privacy is protected. The level of technological expertise of users, which this study defined as the technical skill and comfort level of the user with technology in general, offered an interesting perspective in correlation with user perceptions of privacy.

Generally speaking, the higher the user's technology expertise, the higher the perception of privacy, as illustrated in figure 1. The statement holds true with the exception of users that identified as having "non-existent" technology expertise. This group had a higher perception of privacy than the group of respondents that identified as having low technology expertise. Having a high level of technology expertise indicates that the user is aware of the technology landscape and can navigate technology controls effectively. A conclusion is that users with a high level of technological awareness may feel more comfortable with the controls provided by the device manufacturers or may feel the controls are sufficient and hence have a higher perception of privacy compared to the other groups.

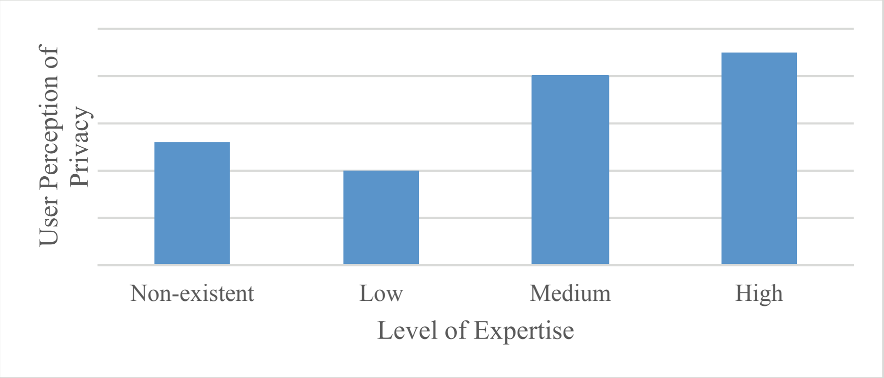

Figure 1 - User perception of privacy by the level of technology expertise

Do VBA privacy perceptions vary based on smartphone adoption?

Research question two examined if users' privacy perceptions of VBAs vary based on their smartphone operating system. The two primary smartphone operating system platforms we considered in this study are Apple iPhone and Google Android. Respondents in the survey were asked to select which smartphone operating system they use. Three options were presented, with the third option as "Other." Respondents that chose "Other" were excluded from the survey as this category could include a wide range of devices from basic to non-Apple or Google smartphones. Google's Android users had a higher mean privacy perception value than Apple iPhone users, as shown in Figure 2. A surprising finding was the correlation between a user's phone type and the user's perception of the privacy of VBAs. Users of Google Android-based smartphones have a higher perception of privacy (confidence that their privacy is protected) than Apple iPhone users. User perception, like in research question one, was broken down into two components: user privacy awareness and trust. Users who had Google Android-based smartphones had a more positive trust factor than users of the Apple iPhone.

Furthermore, with the user privacy awareness variable, Google Android-based smartphone users had a higher awareness factor than Apple iPhone users, as shown in figure 2. This result may imply that users who own an open and less restrictive smartphone like Google Android have somehow been influenced by their devices. As a result, they have a higher perception of the privacy of VBAs relative to users of the Apple iPhone, which is a closed platform.

There were other insightful data points from the research. The correlation between user privacy perception and the technology awareness factor was unique. We observed that the higher the users' privacy perception was across both smartphone operating systems, the higher their technological awareness. We had a consistent result when we analyzed the respondents' phone type relative to the derivative factors of trust and technology awareness, as shown in Figure 2. Android users had a higher level of trust and technological awareness than Apple iPhone users.

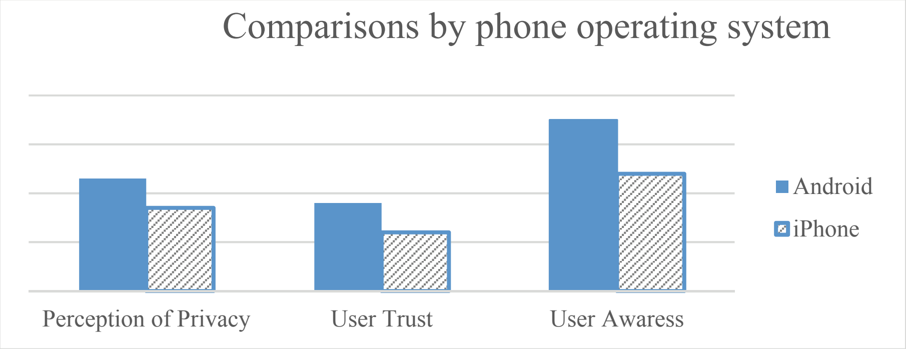

Figure 2 - User perceptions, trust and awareness by phone operating system

Do users' privacy perceptions of VBAs vary based on user demographics?

Research question three examined if privacy perceptions of VBAs varied based on user demographics. Female VBA users have a higher perception of privacy than males, as shown in Figure 3. Users above the age of 51 have a significantly lower perception of privacy than users in the 18-25 and 36-50 age brackets. Users in the 25-35 age bracket have the lowest perception of privacy, as shown in Figure 4.

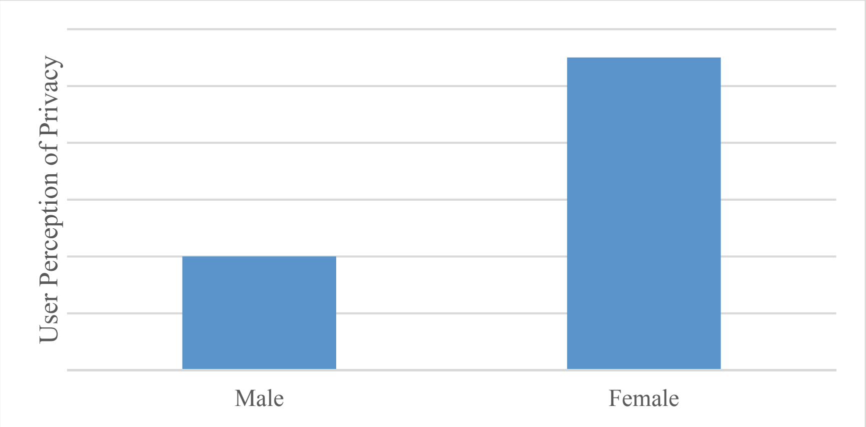

Figure 3 - User Perception of Privacy by Gender

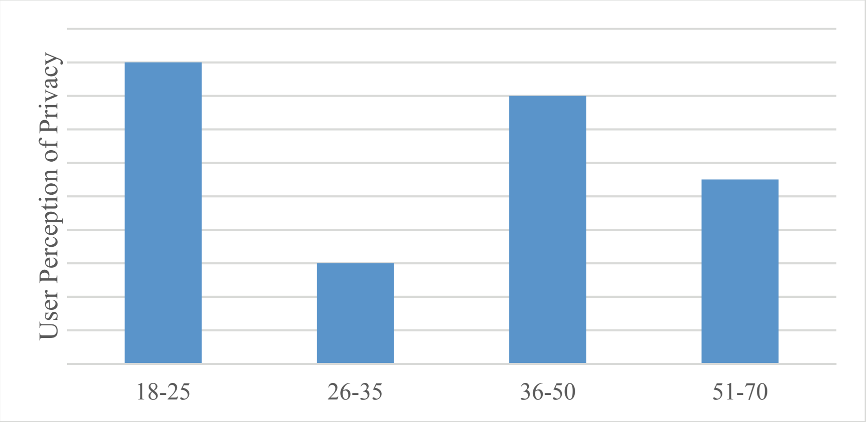

Figure 4 - User Perception of Privacy by Age Range

Respondents with a high school degree have a higher perception of privacy, followed by respondents with a master's degree. Respondents who identified as having "some college but no degree" ranked close to respondents with a master's degree. The two groups of respondents that ranked 4th and 5th were those with a bachelor's degree and those with an associate degree. Also, doctoral degree holders have the lowest perception of privacy compared to other academic levels. Details are included in figure 5.

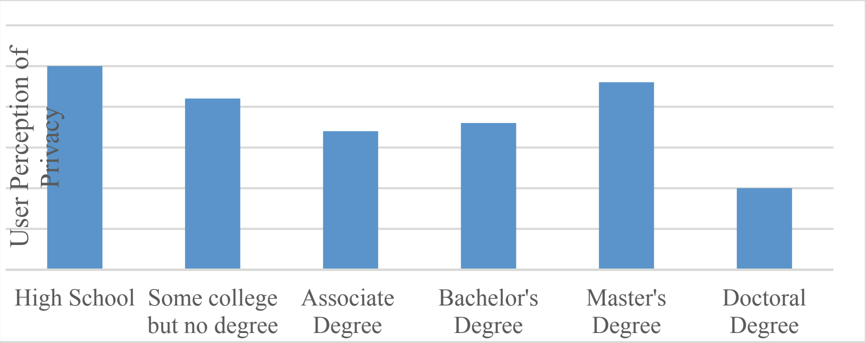

Figure 5 - User Perception of Privacy by level of education

Conclusions

The ubiquitous and rapid adoption of VBAs like Amazon Alexa and Google Home by people around the world, either through interaction with these devices physically or with a mobile application, has raised questions about the privacy of the devices. Primarily because of how close the devices are to the users. Privacy considerations for VBAs are fluid based on two factors. First, the roles and services provided by VBAs are constantly changing. On a regular basis, more devices and services are VBA capable. These changes will affect the adoption, usage, and privacy concerns with VBAs. Secondly, the changing cybersecurity landscape affects privacy users' perceptions. Specifically, has the user suffered a data theft of their own PII from a VBA? If so, perceptions of privacy will differ from users without a VBA-related data breach. Perceptions will also change over time as VBAs evolve over time and offer different technical controls.

The study shows that the higher the user's trust of VBAs, the higher the user's perception of the privacy of VBAs. Also, the higher the user's awareness of privacy and security controls of the VBA, the higher the user's perception of privacy. Awareness ranked the highest in terms of factors that influence user perception of privacy as compared to trust. Female participants have a higher perception of privacy compared to their male counterparts. Also, VBA users of the age group of 18-25 and 36-50 have a significantly higher perception of privacy compared to users in the 50-70 age group. The major difference in academic level and privacy perception is that Doctoral degree holders have a significantly lower perception of the privacy of VBAs.

Technology expertise of users, which this study defined as the technical skill and comfort level of the user with technology in general, offered an interesting perspective in correlation with user perception of privacy. Users that identified as having high technical expertise have a higher perception of privacy for VBAs. The level of user perception of privacy reduces with the technical expertise level. This is an indication of the awareness factor of the user. A high technical awareness of a user signifies a high perception of privacy, and a low technical awareness signifies a low perception of privacy.

The results offer an interesting and surprising perspective on users' perceptions of privacy relative to their smartphone devices. Why do users of Android devices have a higher perception of privacy and awareness as compared to iPhone users? Could the granular controls, customizable operating system, and the non-sandboxed nature of Android devices influence the participant's mean privacy perception? This could be an area for future research.

Limitations

This study explored the factors that could affect privacy perceptions of VBAs. While the study included global respondents, the majority were U.S. based. Therefore, this study may not have captured cultural or national differences. The survey instrument was written in English as the distribution was originally intended for participants who live in the US. The analysis of the results indicates that some of the LinkedIn participants were residents in other parts of the world where the participants' first language may not be English; this has the potential to cause a significant survey burden. Also, for the data to be representative of the global population, the survey should be written in the primary language of the location the survey is being distributed.

Another limitation is concerned with the demographic of the participants. The scope of the participants did not include respondents who may be economically disadvantaged. Since the scope of the data collection is tilted toward the participants who had a basic education and at least above minimum wage earnings. Future research could enrich the dataset and results by including under-represented participants.

The study also examined only two VBAs, Amazon Alexa and Google Home, so the results may not be generalizable to all VBAs. The second limitation of this study is the language used in the survey instrument. Lastly, the study was non-longitudinal, so the recency of a data breach may affect future privacy perceptions.

Areas of Future Work

To address these limitations, future work should consider how to measure how VBA privacy perceptions vary over time with the same group of users. A cohort-based longitudinal study could then track differences in perceptions between users who had suffered a VBA-related privacy breach and those who had not. It could also measure how the perceptions change post-privacy breach. Fortunati et al. (2022) examined the gender personification of VBAs along with their verbal cues and found that over 80% of men and women in the U.S. and Italy viewed Alexa as female. They also investigated whether the respondents viewed Alexa as an inferior, equal, or superior communicator. Half of the respondents said Alexa was an inferior communicator. Only in Italy was there an association with inferiority and being female. Interesting future research would be to explore if there are relationships between levels of trust and the perceived gender of the VBA device. This is another area for future research.

References

Atluri, I. (2017). Managing the risk of IoT: Regulations, frameworks, security, risk and analytics. ISACA Journal, 3(1), 19-26.

Awojobi, B., & Chang, H. (2017). Security and privacy issues with smart thermostats – A first look. https://digital.library.unt.edu/ark:/67531/metadc1036560/m2/1/high_res_d/Biodun_Awojobi.pdf

Brown, S. (2019). Most Americans don't think it's possible to keep their data private, report says. https://www.msn.com/en-us/news/technology/most-in-us-don-t-think-it-s-possible-to-keep-data-private/ar-BBWUn0z?ocid=anaheimntp

Thousands of Amazon Employees Listen to Alexa Voice Recordings. Costello, T. and Guthrie, S. (Directors). (2019, Apr 11).[Video/DVD] New York: NBCUniversal Media, LLC. https://highered.nbclearn.com/portal/site/HigherEd/browse?cuecard=118959

Figliola, P. M. (2020). The Internet of Things (IoT): An overview. (No. IF11239).Congressional Research Service (CRS). https://crsreports.congress.gov/product/pdf/IF/IF11239

Fortunati, L., Edwards, A., Edwards, C., Manganelli, A. M., & de Luca, F. (2022). Is Alexa female, male, or neutral? A cross-national and cross-gender comparison of perceptions of Alexa's gender and status as a communicator. Computers in Human Behavior, 137, 107426. https://doi.org/10.1016/j.chb.2022.107426

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660.

Lueth, K. L. (2018). State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating. https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

Moor, J. (1997). Towards a theory of privacy in the information age. ACM SIGCAS Computers and Society, 27(3), 27-32. https://doi.org/10.1145/270858.270866

Panichas, G. E. (2014). An intrusion theory of privacy. Res Publica, 20(2), 145-161. https://doi.org/10.1007/s11158-014-9240-3

Patel, H. (2017). IoT needs better security. ISACA Journal, 3(1), 27-31.

Poremba, S. (2020). Incident classification patterns and subsets. https://www.verizon.com/business/resources/articles/s/understanding-the-risk-of-botnet-attacks/

Razzaq, M. A., Gill, S. H., Qureshi, M. A., & Ullah, S. (2017). Security issues in the Internet of Things (IoT): A comprehensive study. International Journal of Advanced Computer Science and Applications (IJACSA), 8(6), 383-388.

Saltzman, M. (2018, April 4). Amazon (and Alexa) know a whole lot about you. Here's how download and delete that info. USA Today (https://www.usatoday.com/story/tech/columnist/saltzman/2018/04/04/amazon-and-alexa-know-whole-lot-you-heres-how-download-and-delete-info/482286002/)

Savitsky, L., Illingworth, M., & DuLaney, M. (2009). Civilian social work: Serving the military and veteran populations. Social Work, 54(4), 327-339. https://doi.org/10.1093/sw/54.4.327

Wachter, S. (2018). The GDPR and the Internet of Things: a three-step transparency model. Law, Innovation and Technology, 10(2), 266-294.

Warren, S., & Brandeis, L. (1890). The Right to Privacy. Harvard Law Review, 4(5), 193-220.