Online Media & Society
Vol.7, No.1 (March, 2026), Pp.17-28
ISSN(online): 2790-1882, ISSN(print):2790-1874
DOI: https://doi.org/10.71016/oms/drx1gt19

Original Article **https://hnpublisher.com**

Privacy Concerns in the Digital Age of Smart Homes Assistance: Convenience at What Cost?

Maida Khan[1], Ahsan Raza[2], Maryam Mansoor[3]

[1]Lecturer, Media and Communication Studies, National University of Modern Languages, Islamabad, Pakistan.
[2]Lecturer, Media and Communication Studies, National University of Modern Languages, Islamabad, Pakistan.
[3]Lecturer, Media and Communication Studies, National University of Modern Languages, Islamabad, Pakistan.
Correspondence: maidakhan@numl.edu.pk[1]

ABSTRACT

Aim of the Study: The smart devices are also making their way into Pakistani homes with automation, efficiency, and convenience. Nonetheless, there are also other types of domestic surveillance and data vulnerability with the introduction of new technologies. The paper explores the way in which users of smart home gadgets in Pakistan understand and bargain privacy in their daily settings.

Methodology: Based on the semi-structured interviews of ten users of smart devices in their homes, the study examines personal experience, perceived risk, and privacy management strategies emerging as a result of the implementation of the Internet of Things (IoT) technologies in the home environment (Magara & Zhou, 2024). As a qualitative and thematic design, the respondents were chosen according to the frequent use of the smart devices, such as smart cameras, voice assistants, home automation systems, as well as remote security applications. A thematic analysis was done through inductive analysis to transcribe and analyze interview data.

Findings: Results show that the participants have a technological convenience paradox and an augmented exposure to surveillance, whether it is internal (within the household) or external (corporate, governmental, and hacker threats). Digital literacy was displayed differently by the users, who conditioned their consciousness of the data collection processes and their privacy management ability. Placing devices and choosing which ones to use was one of the strategies as well as password control and avoiding some features.

Conclusion: The researchers come to the conclusion that smart gadgets transform domestic privacy borders in Pakistani families exposing the new issues of trust, control and data management. These results demonstrate the necessity of raising the public awareness, making policies culturally aware, and designing technologies that users can use to lessen the privacy risks related to the adoption of smart homes.

Keywords: Interactive Devices, Surveillance, Digital Assistance, Smart Homes, Privacy Management Theory, User Behavior.

Article History

Received:
October 23, 2025

Revised:
January 31, 2026

Accepted:
February 06, 2026

Online:
February 16, 2026

1. INTRODUCTION

The technologies of smart homes are coming to prominence in the daily lives of people worldwide. The way people are using these smart technologies for locking the doors, as voice assistants, cameras, and to automatically switch on and off appliances is making homes safer and more efficiently controlled. These technologies have links to the internet and gather data to execute tasks automatically, react to commands, and provide the users with the opportunity to control their houses remotely. To most individuals, this gives them a feeling of contemporary comfort and power. But these devices are also bringing concerns regarding privacy, surveillance, and security of information, as they enter domestic areas (Guhr, et al., 2020).

Safety and protection are the main aspects of smart home that are discussed. An intelligent camera can assist a homeowner to monitor what is going on when he is away and an intelligent lock will provide a notification in case someone is attempting to open the door. These characteristics can ease the fears and boost the feeling of security in the home. However, the same gadgets which safeguard can also spy on, record, and save on the activity in the home (Waheed, et al., 2023). Voice assistants can be used to listen to instructions, but also capture sound information. Cameras can be used to record daily activities. Such features are something to think about the extent of information sharing with whom and to what end.

Internet of Things Technology (IoT) has led to the rapid adoption of intelligent domestic devices that have radically changed the domestic functionality, providing high levels of automation, connectivity and convenience. Nonetheless, there is a severe price on the privacy of the user of these innovations. Connected household gadgets status quo gather huge portions of private information-user behavioral norms, GPS positioning and user identification-often without any open disclosure and without any express permission of the individual user (Aswar, et al., 2025).

Though the use of smart homes is dominant in the western nations, there is also increased demand for the use of smart devices in developing countries. Residents of urban areas in Pakistan are increasingly adopting smart technologies, particularly among the middle and high-class families. There is a popularity of imported home automation systems, application-based security applications, and locally based CCTV. The security factor, the wish to keep an eye on homes whenever one is not at home, or just enjoy the comfort of living in the modern world, are some of the reasons why many people are using smart devices. Younger generation is more inclined towards the use of digital tools and automation (Milan, et al., 2015).

Smart homes are expected to enhance the living standards of people. Nonetheless, they are storing immense personal and sensitive information and hence the need to protect the privacy is of paramount importance (Bugeja, et al., 2021). Nonetheless, Pakistan is a different case when it comes to the perception of smart home applications. There is still a lack of awareness of digital privacy in society, and laws on the protection of national data are still developing. Consumers do not always comprehend the level of information that smart devices gather as well as how such data can be utilized by companies and platforms. Alongside, there is a digital disparity between households. Certain users can handle device settings or privacy, whereas other users can use default settings without questioning it.

In Pakistani homes, privacy is also a cultural and social factor. The home is a personal and secure space, but has to be shared with the family members, relatives, guests, and domestic workers. The smart devices can alter the privacy management in these relations. As an example, a household worker or a child can be monitored with surveillance cameras, or someone outside the home can be able to see what is going on at home using a remote access. It is based on these practices that privacy in smart homes is not limited to the digital information but rather ordinary interactions and limits.

The research on privacy in Pakistani smart homes has three principal reasons that are significant. To begin with, it is on the rise in adoption, and how individuals perceive privacy can aid in determining upcoming challenges. Second, the studies on smart homes have been limited in Pakistan, particularly from the perspective of the everyday users. The majority of discussions that exist are concerned with

technology, infrastructure, or market trends, but not lived experiences. Third, the matter is related to more general concerns, including digital rights, consumer protection, surveillance, and trust.

The paper concentrates on the understanding of privacy by Pakistani users of smart devices in their everyday lives. It examines how privacy is perceived by them, the issues that they might be worried about, and the ways in which they attempt to resolve them. The paper employs semi-structured interviews with ten users of smart home to explore these questions. Interviews enable the participants to explain their experiences, motivation and anxiety using their own language, and these are also informative and cannot be easily captured by the use of surveys.

This study will help create a more solid picture of the role of smart technologies in transforming domestic life in Pakistan since user views will be analyzed. Debates on privacy cannot be left to the technical professionals and policy makers but also the individuals that come into contact with these technologies on a daily basis as the concept of smart home continues to grow. Even though smart devices seem convenient and secure, they give rise to new questions concerning control and trust, as well as the limits of personal information. This paper has examined the way that users are processing these changes and the way that privacy is being bargained within the contemporary Pakistani house.

1.1 Problem Statement

The high rate of the introduction of smart home devices in Pakistan has introduced new conveniences, efficiencies, and types of digital control over the home environment. Nevertheless, the move to interconnected living has also raised concerns with acuity on the way personal information is created, distributed, and possibly misused. Although users will enjoy improved security, automation, and comfort, most of them do not understand how these gadgets gather data, the people who can access such data, and how they can ensure their privacy. In an environment where formal data protection legislations are still immature, there exists an unequal spread of awareness regarding the threat on privacy, which has been prevalently overridden by the temptation of technological convenience.

Current studies of smart homes are mostly directed towards Western societies, sophisticated technological markets, and institutional paradigms of privacy. Little has been done to address the issues of privacy concerns in the normal households of Pakistan, where the cultural norms, family setup, and informal security practices influence the usage of technology in unique ways. With the infiltration of smart devices in middle-class and urban households, the knowledge about how digital surveillance is perceived and dealt with by Pakistani users in the privacy of the domestic environment is becoming even more of a gap. This gap explains why empirical investigation of how users of smart homes perceive the risks to privacy and apply coping mechanisms during the process of negotiating between comfort, safety, and control is necessary.

1.2 Significance of Study

This study leads to scholarly research and community knowledge in a variety of ways. To begin with, it is one of the few qualitative studies of smart home privacy in Pakistan, a context that is generally not mentioned in the global discourse on digital surveillance. By addressing the daily users, it puts emphasis on the lived experiences, issues, and management practices that determine how individuals cope with new technologies in household settings.

Second, the research has a social and cultural implication. Smart homes are not autonomous, as they overlap with domestic stratifications, gender roles, security fears, and general relations of trust. The knowledge of such intersections can assist in the visualization of the ways of privacy negotiation between users and companies, as well as family members, visitors, and home workers.

Third, the results provide useful information on policymakers, technology firms, and consumer education initiatives. Pakistan is on the path to becoming more digitalized, and safe and informed technology usage has to be supported urgently. The research can find out what the community needs to treat with greater

clarity, what privacy, and what sensitization would help guarantee that technological innovation does not hurt individual rights and domestic peace.

Lastly, the research provides the basis of future academic research on smart homes in the South Asian settings and stimulates the comparative, interdisciplinary, and longitudinal studies in the field, where the expansion is highly expected.

1.3 Research Objectives

1. To investigate how users of the smart-home conceptually understand and express privacy issues in their daily lives.
2. To explore the approaches and measures that people take to overcome privacy threats when technologies of smart homes are utilized.

1.4 Research Questions

RQ1: What is the experience and perception of privacy among the Pakistani society who use smart devices at home in their daily lives?

RQ2: What are the methods smart home users adopt to keep a balance between assistance and invasion of privacy?

2. LITERATURE REVIEW

The smart home is regarded as one of the primary features of the next-generation Internet, and a considerable proportion of houses become smarter by implementing the Internet of Things (IoT) technology to improve the security of their homes, energy efficiency, and comfort. At the same time, the issue of privacy introduction into the IoT space has also been reported as one of the main barriers to the realization of the smart home vision (Jacobsson & Davidsson, 2015). Privacy issues are a concern in various contexts. Smart devices applied to a smart environment are one such context. Such developments are being adopted by people creating more and more information, which is usually created without their knowledge, or they are fully aware of what they are getting themselves into when sharing and using such gadgets (Arabo, et al., 2012).

Smart homes can be connected through Internet-based devices (lights, locks, cameras, thermostats, TVs, refrigerators, voice assistants, etc.) to automate functions and make it more convenient. Within the last decade, these technologies have been integral parts of the household in most parts of the world and have developed due to the emergence of AI, voice recognition (e.g., Amazon Alexa, Google Assistant, Apple Siri), and Internet of Things (IoT) platforms (Beazley, 2024).

Owners are also citing high positive returns: in one study 77% of adopters said that smart devices made their lives better, primarily by providing greater security (cameras, smart locks), remote monitoring (setting adjustments remotely), convenience (convenience), and savings in energy (Arbanas, et al., 2023). Adoption is rising rapidly. Indicatively, as of 2019, Amazon was selling more than 100 million devices with Alexa, and an estimated 1 in 5 adults in the U.S. already had a home voice assistant (with Alexa controlling about 70% of the market) (Lynskey, 2019). According to reports by the industry, the market is estimated to be more than 100 billion dollars in 2023, but with a multi-fold growth projected by 2030 with the help of AI-enabled cameras, assistants, and connected appliances (Hill, 2025).

Smart home technology, also referred to as a home automation system, enables the homeowner and the residents to manage and monitor the smart devices such as heating, ventilation, and air conditioning (HVAC), refrigerators, doors, cameras etc. These features make the users easier as they offer a secure and appropriate environment. Nonetheless, simultaneously these intertwined devices might be used by maleficent criminals because of the disregard of the default security and privacy issues of these devices (Iqbal, et al., 2022).

The Internet of Things (IoT) is a network of smart devices that are capable of listening and talking to each other. These attached devices will be 38.6 billion in 2025 and gadgets are gathering information on your location, contacts, calendar events, smart homes, health devices, and so on. There are several security and privacy issues that come about owing to its heterogeneity and usage. It is significant that the challenges and problems are identified to enhance security and privacy (Abid, et al., 2022).

Smart home conveniences have big privacy disadvantages. Practically every device gathers information about habits, speech, preferences regarding media, location, and layout of the home of the residents. Analysts are concerned that the primary goal of smart devices is to read us more and sell us more (Beazley, 2024). The risks are numerous and well-documented: the voice assistants are created to be always-listening, cameras and smart TVs are capable of taking pictures of your everyday mode of existence, and networked devices can be vulnerable to attacks on their security measures to enable eavesdropping. To take an example, the National Cyber Security Centre in the UK has advised owners of smart-cameras and baby-monitors to secure their settings on multiple occasions, and the FBI has also threatened that certain smart television sets will listen to and spy on users by default. (Winder, 2020).

The key findings of a study conducted in (2025) demonstrate that though users are more conscious of the potential risk privacy can present, there is a great gap in their capacity to put these challenges into proper focus since their awareness is limited, their devices resources are insufficient, and they do not have confidence in the manufacturer. The review raises pertinent issues, including data over-gathering, lack of transparency and poor security which add up to amplify user vulnerability to misuse and data breaches (Aswar, Aet al., 2025).

Misconfigurations are reported in the media: in one instance, a misconfigured Amazon Echo uploaded 1,700 private audio snippets to an unknown person; in another case, older people have been shocked to discover recordings or videos of strangers being captured by their equipment (Lynskey, 2019). These anxieties are expressed in public attitudes. According to polls and media coverage, no amount of privacy in smart homes is a concern. A poll revealed that a phobia of unintended recording by their gadgets (e.g., Alexa overhearing personal conversations) is a concern to 59% of smart-speaker users (Winder, 2020).

The popularity of smart home devices (SHD) has raised more privacy concerns among users, although they do not have user-friendly controls. Although much research has been done to comprehend the issue of privacy and threat models of SHD users, not much research has been done yet to inform the development of privacy controls in SHDs (Chhetri & Motti, 2022). Therefore, this research will add knowledge about how users see and manage privacy in smart homes and how they keep the balance between assistance and invasion of privacy.

The development of smart home devices has transformed the modern way of life by making life more convenient, automated and economical. These advantages however come at the price of huge privacy and security issues. A study conducted by Hussain (2025), pointed the tension between use and security concerns linked with smart devices, and the importance of awareness among users, and the necessity of standardized measures to ensure it. She also suggested sealing the loopholes in the enforcement of security and preserving privacy to provide a safer smart home environment (Hussain, 2025).

2.1 Theoretical Framework

One of the main concerns now that smart home technologies are coming into the domestic environment is privacy, gathering, storing, and transmitting personal information. Inconveniently, gadgets like voice assistants, surveillance cameras, smart locks, and automated appliances are convenient and secure at the same time, which opens the possibility of being surveilled and exposing data. The key to grasping the nature of the way users manage and experience these privacy predicaments lies in the necessity of a framework that would capture both the interpersonal aspects as well as the technological aspects. Such a lens includes Communication Privacy Management (CPM) Theory (Petronio, 2002) (West & Turner, 2010).

CPM is a conceptualization of the view of privacy as a dynamic, rule-based process and not a fixed state. People consider themselves as the proprietors of personal information and create a boundary to decide who should access their information, on what terms, and in what way to share it. These limits may be individual or group and are formed with the help of trust, relations, and cultural beliefs. CPM has been broadly used to interpersonal communication and online communication to learn how individuals cope with sensitive information in complicated social situations.

CPM can be used in the context of smart homes to understand the process of privacy negotiation between human and non-human actors. The customary privacy limits at home are interpersonal, made by the family members, visitors, or domestic workers. Smart devices add new stakeholders (companies, cloud solutions), and possibly the state authorities, who can access personal data. This complicates ownership, and users have to handle information relationally and technologically.

CPM can be especially applicable to Pakistani families since the homes serve as communal places that can be shaped by gender roles, hierarchies, and trust. Smart devices are capable of challenging status quo, and users are inclined to employ measures that involve setting up of devices, restricting access, educating family members, or managing data. CPM enables such strategies to be perceived as active work to control the flow of information and protect privacy levels.

This research paper employs CPM to understand the meaning of privacy, threats, and information control by Pakistani smart home users in their homes. The theory also brings out perceived vulnerabilities and the strategies of coping and details the nature of privacy as dynamic and negotiated in technology-mediated domestic settings. CPM allows a holistic approach to privacy in smart homes by placing the individual strategies in a wider social and technological context.

3. METHODOLOGY

The research design that was applied in this study was a qualitative research design in order to learn how users of smart homes in Pakistan perceive and control privacy issues in their daily lives. The qualitative research was selected to ensure that the participants' experiences and attitudes, as well as strategies, are captured in detail, which cannot be exhaustively determined using quantitative research (Creswell, 2003). Semi-structured interviews were used to enable the participants to think about whatever they wanted and direct the discussion on privacy, surveillance, and usage of devices.

Purposive sampling was used to select (n=10) participants (see table 1) who had the presence of smart home devices such as security cameras, smart locks, automated lighting, and voice assistants, among others. The respondents were chosen to represent the various household types, ages, and genders in order to get various perspectives. Each of them lived in cities, where smart home penetration is more advanced, and had experience with several devices. The interviews were approximately 25 to 35-minutes in length, held face-to-face and via the internet.

The participation was voluntary, and the purpose of the study was communicated to the participants, who were assured of their rights to withdraw at any time. Anonymity and safe storage of data ensured confidentiality.

Thematic analysis was used to analyze data and identify patterns and themes of the experiences of the participants. It involved being introduced to transcripts, coding meaningful statements, creating themes, and narrowing them down to represent the privacy issues and management approaches in an appropriate manner. The credibility was achieved through the selection of participants with different experiences and by providing summaries of findings to the participants to confirm the results.

Table 1: *Demographics of Respondents (N=10)*

Participants	Gender	Age Bracket	Education	Marital Status
P1	Female	(25-34 years)	Bachelors	Married
P2	Female	(25-34 years)	Masters	Married

P3	Male	(25-34 years)	Bachelors	Single
P4	Female	(35-44 years)	Masters	Married
P5	Male	(25-34 years)	Masters	Single
P6	Male	(35-44 years)	Masters	Single
P7	Female	(35-44 years)	Intermediate	Single
P8	Male	(25-34 years)	Bachelors	Married
P9	Female	(18-24 years)	Bachelors	Single
P10	Male	(35-44 years)	Intermediate	Married

The study is very insightful, but it cannot be described as free of limitations. The limited sample and purposive sampling restrict the generalizability, and the targeting of urban households might not accurately represent the situation in rural settings. The answers given by the participants might also be biased by social desirability or unwillingness to talk about sensitive issues. In spite of such limitations, the study provides some exploratory information regarding the understanding and coping of privacy among those users of smart homes in Pakistan in a developing digital domestic setting.

4. RESULTS

4.1 Knowledge and Discourse of the Privacy Issues around Smart Devices

4.1.1 Surveillance Risk Awareness

The participants showed different degrees of consciousness of the possibility of surveillance by smart devices. Cameras and voice assistants have the ability to gather data that they do not have control over, and many understood that.

> *"I understand that my camera captures everything, even when I am not checking it. I am concerned about who is viewing it, perhaps not any other person, but the company itself." (Participant 3, Male).*

> *"Alexa is very convenient, yet I am not fully aware of where my voice commands are going or if there is any possibility of misusing it. When you think about it deeply, it scares you sometimes." (Participant 7, Female).*

> *"I was not very concerned about the privacy concerns of technology until I had watched a Netflix movie CTRL. It was an eye-opener movie that showed how dangerous over-reliance on technology could be in the future." (Participant 9, Female).*

Such reactions show that customers are aware of internal and external risks of surveillance. Although the devices are perceived to be utilized in the name of safety, members understand that the information can be manipulated by unidentified people, which brings about the feeling of exposure. Consciousness of surveillance seems to drive careful practices although people may still use gadgets because of convenience.

4.1.2 Privacy as a Selective Issue

The issue of privacy was often formulated in connection with domestic workers and relatives. Participants stressed a need to secure some parts and data in the common residential environment.

> *"I only use the camera close to the entrance, but not inside the places where people live, since I do not mean to capture my kids at all times." (Participant 1, Female)*

> *"I even inform the helper about sensitive areas that he must not approach. I do not want him to approach the study where the smart lock is, as it tracks access." (Participant 6, Male)*

> *"It is mostly on us how we keep the balance. We should use the technology rather than allowing it to use us." (Participant 3, Male)*

This theme brings out the fact that privacy of smart home is a relationship and a social bargain. When handling devices, the participants take into consideration the need, rights, and expectations of other household members. The results indicate that privacy control goes beyond data protection, and are also concerned with sustaining trust and integrity in the home.

4.1.3 Convenience over Privacy Threats

Some of the respondents admitted that the privacy issue is frequently replaced by the convenience of smart devices.

> *"Yes, I understand that the devices are collecting information, but it is much more convenient to monitor my house during the working time than be worried about privacy all the time." (Participant 2, Female)*

> *"I do not envision any substantial damage this technology would inflict on me." (Participant 4, Male)*

The responses indicate a practical attitude to privacy. Users voluntarily take a degree of compromising information in exchange of convenience and security perks. This is a trade-off highlighting the fact that the concept of privacy is at best relative and it is a matter of balancing risk and functionality. They do know about the perceived threats but they still need technological aid.

4.2 Practical Measures for Managing the Privacy in Smart Homes of Pakistan

4.2.1 Restricting Access of Devices for Managing Privacy Control

The subject respondents indicated that they have altered the device settings, restricted permissions or have used features selectively to minimize risk exposures to privacy risks.

> *"The way I handle it is by destroying the cloud storage of the camera and simply saving recordings in my phone. In that manner, it cannot be accessed by any other person." (Participant 5, Male).*

> *"I often mute the voice assistant when I do not need it and switch it off at night." (Participant 9, Female).*

These reactions exhibit active interaction with technology. Technical measures are actively used by the participants in order to take back the control of data and minimize the undesired monitoring, demonstrating that the process of privacy management can be integrated into the everyday use of the devices.

4.2.2 Structural and Behavioral Control as a way of Managing Privacy Risks

Privacy was safeguarded by users using place of device and household regulations.

> *"The camera does not enter bedrooms, just in the corridor. That's my rule," (Participant 4, Female).*

> *"The family has come to an agreement, that no one in the family should touch the smart lock codes, except parents." (Participant 8, Male).*

As revealed by structural and behavioral strategies, users compromise their privacy through physical and social organization of their space. The location of the devices and the setting of household rules have also assisted to set the boundaries and restrict unwanted exposure and the relational element to privacy.

4.2.3 Surveillance and Awareness to Minimize Risks Associated with Smart Homes Privacy

The respondents indicated that they were vigilant when it comes to tracking the device usage and software updates.

"I monitor the application on weekly basis to know who watched the camera. It makes me feel like I am in control of it" (Participant 6, Male).

"I read about updates and new settings so that I can uncheck the options I do not trust." (Participant 3, Male).

Continued watchfulness is an indication that users would like to control smart home devices. Through being aware and keeping track of use, participants minimize ambiguity and strengthen their privacy boundaries and the dynamic and adaptive character of privacy management.

All in all, the results point to the fact that privacy issues among Pakistani smart home users are both technological and relationship-related. The users are conscious of the risks of surveillance, yet convenience can tend to influence behavior. Technical adjustment, spatial and behavioral management, communication and vigilance are some of the ways of managing privacy. Both strategies are expressions of an everyday life balancing convenience, safety and control through a negotiable and dynamic approach to domestic privacy.

5. DISCUSSION

This research paper has shown that the issue of privacy in Pakistani smart homes is a complex, dynamic one. Privacy is perceived by users as an aspect that has to be managed as opposed to assumed. They know that there are smart devices like cameras, voice assistants, and smart locks that are able to gather and transfer personal data. Concurrently, they acknowledge the practical value of such gadgets, such as convenience, security, and ease of tracking the happenings in their homes when away. This offers a balancing act at all times between the need to uphold privacy and the benefits of technology. These findings supported the argument by (Aswar, et al., 2025) that people are well aware about the privacy concerns, yet they lack to create a proper mechanism to cope with these challenges due to lack of proper awareness. Also, people are not fully aware of what they are sharing (Arabo, et al., 2012).

Privacy issues did not just revolve around outside threats like having companies access my data, but also relations and social life in the household. Respondents talked about managing the areas and operations with care to accommodate family members, guests, and domestic workers. The location of the cameras, the exchange of access codes to the devices, and regulations regarding which rooms and activities were monitored all represent the continuous process of negotiation of the privacy limits. The household communication turned out to be one of the primary approaches, and the participants were negotiating the rules of privacy, telling the other members about the monitored areas, and accepting the available practices. This point supported the argument by (Hussain, 2025) that people are more inclined towards the advantages they are getting through these technologies at the price of security concerns and privacy threats linked to these technology.

Technical solutions, including the settings of the equipment, turning off voice assistants, and constraining clouds, were very common. A large number of participants were well-engaged in tracking device activity and software downloads to keep their data under control. Such actions emphasize the fact that ensuring privacy is not a one-time operation but a process. The utilization of technology, domestic habits, and the level of comfort in the households by users is dynamic, which indicates that the privacy of the house is contextual and must be negotiated. (Lynskey, 2019) indicated in a research that adoption of smart technologies is rapidly increasing but issues of privacy acts as a barrier and people are not fully aware of what they are sharing indirectly by using these technologies (Arabo, et al., 2012).

It is also found that convenience tends to influence the perception of privacy. Although the dangers of smart home devices were acknowledged, their advantages tended to surpass concerns, which may be interpreted as a practical attitude to the application of technology. All in all, smart home privacy is lived in the context of awareness, control, negotiation, and compromise with users in the creative process of balancing personal, social, and technological. These findings were in line with the suggestions of study conducted by (Hussain, 2025).

The findings of present research study also supported the assumptions of Privacy Management Theory (West & Turner, 2010) that people see privacy as something that is negotiable by allowing to access some features and restricting the others. They feel privacy is something that can be managed. Yet the importance of creating in-depth awareness regarding the privacy concerns cannot be denied.

6. RECOMMENDATIONS

The users should know that it is important to be aware and proactive in management. It is the responsibility of the users to work on their own to familiarize themselves with device settings, restrict access to prevent unwarranted data gathering by the applications, dispose of placements of devices, and discuss with the members of the household the issue of privacy. Such basic routines as switching off voice assistants or checking app usage can help a lot.

Developers of smart home technologies should offer understandable and easy-to-use privacy settings. The presence of features enabling users to easily customize data collection, restrict access, and get alerts to monitor device activity can contribute to creating trust and promoting responsible use. Smart home privacy could be aided by information and education campaigns, which would allow users to make informed choices. Educating and informing households about the use of safe devices, risks, and simplistic digital security may enable them to safeguard their privacy.

Basically, privacy within smart homes is a matter of precautions that are technical, household communication, and individual caution as an individual. The advantages of smart technology can be achieved when people are assisted with the help of clear controls of their devices and feel a sense of security and control over their personal areas.

7. CONCLUSION

This paper has indicated that privacy in Pakistani smart homes is a multifaceted and dynamic process, which depends on both technology and social relations. The end-users know that, being convenient and secure, there are also possible dangers connected with data harvesting and tracking of smart devices. The consideration of privacy issues is not just about external risks, but also about the establishment of a range of boundaries in the house, reconciliation of family needs and expectations, guests, and domestic employees.

Participants have been shown to actively regulate their privacy through the use of a mixture of technical adaptations, structural configurations, home regulations, communication, and vigilance. They show that privacy does not exist as a given but is rather a dynamic process that needs constant consideration, bargaining, and adjustment. Simultaneously, the perceived convenience and utility of the smart devices can also prompt people to consider some of the risks, which is a pragmatic attitude towards the use of technology.

In general, this research demonstrates that the privacy of smart homes is a fine line between control, comfort, and trust. Users are resourceful in their approach to technological and social issues, and they create individualized approaches to secure their information as they benefit from smart technology. These lessons indicate the need to create awareness of privacy, offer convenient controls on smart devices, and promote honest communication at home. The views of the user regarding the accessibility of their smart home data are based on the perceived usefulness of third parties outside of the home that design, monitor, control, or administer IoT devices and their data. The users also presume that they are safe due to the belief that the manufacturers of IoT devices place the security of their data in distinct hands and do not know the possibility of machine learning inferences that might expose sensitive information, even when no audio/visual data is present (Zheng, et al., 2018).

Finally, given that smart home technologies are continually becoming more popular in Pakistan, it is imperative to learn the ways that users perceive, negotiate, and manage privacy. By understanding privacy as an active process, a relational process, and a contextual process, households, technology

developers, and policy makers can be able to design an environment where technology can positively affect everyday life and not negatively affect the privacy of the individual and the family.

Acknowledgements

None.

Conflict of Interest

Authors declared NO conflict of interest.

Funding Source

The authors received NO funding to conduct this study.

ORCID iDs

Maida Khan [1] https://orcid.org/0009-0002-5433-5140
Ahsan Raza [2] https://orcid.org/0009-0006-9322-4450
Maryam Mansoor [3] https://orcid.org/0000-0002-0072-7811

REFERENCES

Abid, M. K., Qadir, M., Farid, S., & Alam, M. (2022). IoT Environment Security and Privacy for Smart Homes. *Journal of Information Communication Technologies and Robotic Applications*, *13*(1), 15–22. doi:10.51239/jictra.v12i2.307

Arabo, A., Brown, I., & El-Moussa, F. (2012). Privacy in the Age of Mobility and Smart Devices in Smart Homes. *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing* (pp. 819-826). Amsterdam, Netherlands: IEEE. doi:10.1109/SocialCom-PASSAT.2012.108

Arbanas, J., Silverglate, P., Hupfer, S., Loucks, J., Raman, P., & Steinhart, M. (2023). *Consumers make their homes smarter, with a focus on security.* United States: Center for Technology, Media and Telecommunications.

Aswar, S., Adhikari, P., Ahire, B., & Anpan, A. (2025). Public Opinion on Privacy Concerns in Smart Home Devices. *SSRN*, 1-8. doi:https://dx.doi.org/10.2139/ssrn.5220515

Beazley, J. (2024). *Is my home spying on me? As smart devices move in, experts fear Australians are oversharing.* London: The Guardian. Retrieved from https://www.theguardian.com/technology/2024/feb/11/is-my-home-spying-on-me-as-smart-devices-move-in-experts-fear-australians-are-oversharing#:~:text=Share

Bugeja, J., Jacobsson, A., & Davidsson, P. (2021). PRASH: A Framework for Privacy Risk Analysis of Smart Homes. *Sensors*, *21*(19), 1-29. https://doi.org/10.3390/s21196399

Chhetri, C., & Motti, V. G. (2022). User-Centric Privacy Controls for Smart Homes. *Proceedings of the ACM on Human-Computer Interaction*, *6*(CSCW2), 1-36. doi:https://doi.org/10.1145/3555769

Creswell, J. W. (2003). *Research Design Qualitative, Quantitative, and Mixed Method Approaches* (2nd Edition ed.). Thousand Oaks/ London/ New Delhi: Sage Publications.

Guhr, N., Werth, O., Blacha , P. H., & Breitner, M. H. (2020). Privacy concerns in the smart home context. *Discover Applied Sciences*, 1.12. doi:https://doi.org/10.1007/s42452-020-2025-8

Hill, S. (2025). *Here's What the 'Matter' Smart Home Standard Is All About.* New York: WIRED. Retrieved from https://www.wired.com/story/what-is-matter/#:~:text=a%20given%20that%20they%20will,logo%20to%20find%20compatible%20devices

Hussain, D. (2025). PRIVACY AND SECURITY IN SMART HOME DEVICES: CHALLENGES, SOLUTIONS, AND FUTURE DIRECTIONS. *Computer Science Bulletin, 8*(1), 33-43. doi:https://doi.org/10.71465/csb144

Iqbal, W., Abbas, H., Rauf, B., Bangash, Y. A., Amjad, M. F., & Hemani, A. (2022). PCSS: Privacy Preserving Communication Scheme for SDN Enabled Smart Homes. *EEE Sensors Journal*, 17677-17690. doi:10.1109/JSEN.2021.3087779

Jacobsson, A., & Davidsson, P. (2015). Towards a model of privacy and security for smart homes. *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)* (pp. 727-732). Milan, Italy: IEEE. doi:10.1109/WF-IoT.2015.7389144

Lynskey, D. (2019). *'Alexa, are you invading my privacy?' – the dark side of our voice assistants.* London: The Guardian.

Magara, T., & Zhou, Y. (2024). Internet of Things (IoT) of Smart Homes: Privacy and Security. *Journal of Electrical and Computer Engineering*, 1-17. doi:https://doi.org/10.1155/2024/7716956

Milan, K., Zuzana, H., Tibor, N., & Sona, N. (2015). The using of and Attitudes toward Internet and Information and Communication Technologies in Different Age Groups. *Journal of Current Issues in Media & Telecommunications, 7*(3), 269.

Waheed, N., Khan, F., Mastorakis, S., Jan, M. A., Alalmaie, A. Z., & Nanda, P. (2023). Privacy-Enhanced Living: A Local Differential Privacy Approach to Secure Smart Home Data. *International Conference on Omni-layer Intelligent Systems (COINS)* (pp. 1-6). Berlin, Germany: IEEE. doi:10.1109/COINS57856.2023.10189261

West, R., & Turner, L. H. (2010). *Introducing Communication Theory Analysis and Application* (4th ed.). New York: McGraw-Hill.

Winder, D. (2020). *How to stop your smart home spying on you.* London: The Guardian.

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User Perceptions of Smart Home IoT Privacy. *User Perceptions of Smart Home IoT Privacy. 2*, pp. 1-20. New York: Association for Computing Machinery. doi:10.1145/3274469