Issues in Information Systems
Volume 26, Issue 4, pp. 17-24, 2025

DOI: https://doi.org/10.48009/4_iis_2025_102

A privacy metric model for IoT for homes (smart homes)

Nooredin (Noory) Etezady, *Robert Morris University, etezady@rmu.edu*
Ping Wang, *Robert Morris University, wangp@rmu.edu*

Abstract

The proliferation of Internet of Things (IoT) has exponentially increased consumers data collection through device sensors. IoT adds convenience to people's life. However, it poses new security and privacy challenges. Prior research has shown that many consumers do not have sufficient information on IoT. There are some consumers that have enough information but rarely take any action to protect their personal information, which is attributed to the cognitive gap between attitude and actual behavior. Privacy metrics help users understand the level of privacy protection of their devices and motivate them to configure their privacy features. Several studies have called for more research on privacy metrics and the need to focus on identifying and developing new metrics for IoT and smart homes as a step toward user privacy protection. As a first step to develop privacy metrics for IoT and smart homes, this paper builds on prior privacy research to develop a privacy model, which can be used to develop privacy metrics. This model will be developed based on analysis and synthesis of existing research on privacy and IoT for homes.

Keywords: privacy, privacy model, privacy metric, IoT, Internet of Things, smart home

Introduction

As Lowry, Dinev, and Willison (2017) noted, the internetworking of numerous physical devices, which is called the Internet of Things (IoT), is expanding rapidly, extending platforms, and jeopardizing the security and privacy of people and organizations. Most of the IoT devices, ranging from passive RFID chips to home automated applications, utilize wireless signals to connect to networks across the globe. Wireless architecture is based on protocols with vulnerabilities. The IoT devices provide new opportunities for attackers such as spying on someone through their refrigerator or stove oven or turning off a home thermostat causing damage by burst pipes because of overnight freezing. Therefore, compromised IoT can inflict damage on the physical security and well-being of people as homes are becoming a part of various networks. In addition, the large amount of data collected on people's behavior through IoT devices is of concern to consumers. The security and privacy vulnerabilities associated with the IoT device can almost impact everyone (Lowry, Dinev, & Willison, 2017; Protick, 2024).

Although most of the existing literature acknowledges the importance of understanding privacy perceptions, privacy perception has not been addressed by research (Karwatzki, Trenz, & Veit, 2022). Dinev, Xu, Smith, and Hart (2013) noted that although privacy has been studied for many years in various fields such as social sciences, law, economics, psychology, management, marketing, and management information systems, there is not a clear understanding of what it means so that it can be articulated clearly. A clear, measurable, and empirically testable definition of privacy is needed for development of governmental and organizational management policies and practices that protect the privacy and security of people (Dinev et al.). Various research studies have called for more research on privacy metrics and the need to focus on identifying and developing metrics for IoT and smart homes as a step toward user privacy protection. (Bugeja, Jacobsson, & Davidsson, 2020; Vemou & Karyda, 2018; Haug, Lanza, & Gewald, 2021).

This study will synthesize prior studies to develop a privacy model that can be utilized in advancing privacy metrics for smart homes and IoT. This paper's contribution will be a smart home privacy model that can be used to develop privacy metrics for IoT for home (smart home) devices. The paper continues with literature review followed by the research approach and methodology, and privacy model. The paper will end with discussions and implications for this study, its limitations and future areas of study, and conclusion.

Literature Review

Security and privacy are abstract concepts and outcomes of various legal, cultural, and organizational rules (e.g., policy) that are affected by culture and jurisdiction. These concepts are created by humans who can consider them as important or not (Lowry, Dinev, & Willison, 2017). A clear, measurable, and empirically testable notion of privacy is needed for guiding law making and developing privacy and security policies in governments and organizations (Adrito, 2024; Dinev et al., 2013).

Dinev, Xu, Smith, and Hart (2013) consider privacy as a state and the empirically testable definition of privacy as 'perceived (state of) privacy'. Therefore, information privacy may be defined as a self-assessed state that provides the outsiders with limited access to the person's information (Dinev, et al.). Privacy has been defined by some researchers as multidimensional, context dependent, elastic, and dynamic since it changes with life experience (Dinev et al., 2013; Karwatzki et al., 2022). However, the majority of the work has considered it in a single dimension.

Privacy is difficult to measure. For measuring privacy, primarily, privacy related proxies such as privacy concerns and privacy risks are employed in empirical research (Karwatzki et al., 2022; Smith, Dinev, & Xu, 2011). Privacy risk can be defined as the degree that one believes negative outcome may result from known/unknown or authorized/unauthorized access to the individual's personal information (Karawatzki et al.). As Karwatzki et al. (2022) noted, various surveys indicate that users perceive a broad spectrum of privacy risks when using digital services. Privacy risks range from unwanted impact of marketing to constant surveillance and discrimination by third parties. Users' perceived risks influence users' desire to use digital services. Most studies conceptualize privacy risks as a unidimensional construct that refers to a general potential for loss without specifying the cause or nature of the loss.

Research on privacy perceptions focuses on other constructs such as privacy protection, privacy awareness, privacy invasion, privacy control, privacy self-efficacy, and privacy experience, which help to understand the key privacy concerns of individuals. However, these constructs are either unidimensional or study organizational practices and thus do not provide insight into specific individual perceived risks (Karwatzki et al., 2022).

Other studies consider users' privacy concerns for how their personal information is used by others. The benefit of considering privacy concerns of users is that it helps to recognize the importance of multidimensional privacy constructs. Multidimensional privacy constructs facilitate understanding of users' perceptions of the behavior of data collectors. (Karwatzki et al., 2022). However, they do not provide specific consequences of access to personal information, or the particular privacy risk perceived by individuals.

Review of the existing privacy conceptualizations indicates that privacy is a complex phenomenon. And the concepts that are associated with privacy need to be explained. In addition, privacy risks are primarily used to explain information privacy (Karwatzki et al., 2022). However, the nature of privacy risks across various digital services and settings is not well understood. Karwatzki et al. (2022) noted that privacy risk is a multidimensional concept and understanding of specific privacy risks is dependent on the context and situation of a specifically implemented technology. Karwatzki et al. proposed and developed a measurement model for assessing privacy risks by breaking down the concept of privacy risks into its constituting elements. Evaluating privacy risks multi dimensionally provides insights outside of the privacy domain. Acknowledging and evaluating multiple dimensions of privacy risks allows researchers to look closer and add to the realism in empirical models.

The instrument developed by Karwatzki et al. (2022) allows researchers to examine multidimensional privacy risks in their specific research area, as the nature of privacy risks may differ across contexts. Different contexts may put individuals at different specific privacy risks and cause context specific potential losses. For instance, someone using online banking is exposed to a different type of risk and potential loss (e.g., financial loss) than someone who is using social media (e.g., change in peer group perception or negative impact on career prospects). The privacy risks measurement construct developed by Karwatzki et al. with seven dimensions helps in deriving a more accurate and full view of privacy perceptions across different contexts based on privacy risks. These seven privacy-specific dimensions are: physical, social, resource-related, psychological, prosecution-related, career-related, and freedom-related consequences. The developed multidimensional privacy risks measurement scales were tested for reliability and validated by Karwatzki et al.

The study by Dinev et al. (2013) provided empirical support that perceived information control and perceived risk affect privacy perception. Information control is attained by anonymity, secrecy, and confidentiality. Perceived information control affects perceived privacy positively. Factors that are used in perceived risks assessment include information sensitivity, perceived benefits of information disclosure, importance of information transparency, and regulatory expectations associated with information disclosure. Dinev et al. showed that perceived benefits from information disclosure decreases perceived risk. Also, perceived risk substantially increases by the sensitivity of disclosed information, the users' regulatory expectations, and the importance of information transparency. From a practical point of view, it is important to note that privacy risk perceptions and perceived information control are important factors in forming users' privacy perceptions and can be used by device manufacturers to address privacy issues by reducing perceived risks and increasing users' information control.

This study will synthesize the multidimensional privacy metric research by Karwatzki et al. (2022) and the research on privacy perception by Dinev et al. (2013) to develop a privacy model that can be used to devise privacy metrics for IoT and smart home devices.

Methodology and Privacy Model Design

The privacy model for this research is based on the Dinev et al. (2013) definition of privacy. Dinev et al. defines privacy as perceived state of privacy. Perceived privacy is affected by perceived information control and perceived risk. In this model privacy risk and information control affect perceived privacy, which subsequently impacts information disclosure. Information control is attained by anonymity, secrecy, and confidentiality (Dinev et al., 2013). Information control affects privacy perception positively. Privacy is multidimensional and context dependent (Karwatzki et al., 2022). The privacy model for this research takes into account seven privacy specific risk dimensions (physical, social, resource-related, psychological, prosecution-related, career-related, and freedom-related consequences). These seven privacy-specific risk dimensions are explained in table 1.

The factors that affect privacy risks are information sensitivity, importance of information transparency, and regulatory expectations associated with information disclosure, and perceived benefits of information disclosure. Perceived risk increases greatly by information sensitivity, importance of information transparency, and regulatory expectations associated with information disclosure. On the other hand, perceived risk decreases with perceived benefits of information disclosure (Dinev et al., 2013). The derived privacy model is shown in Figure 1.

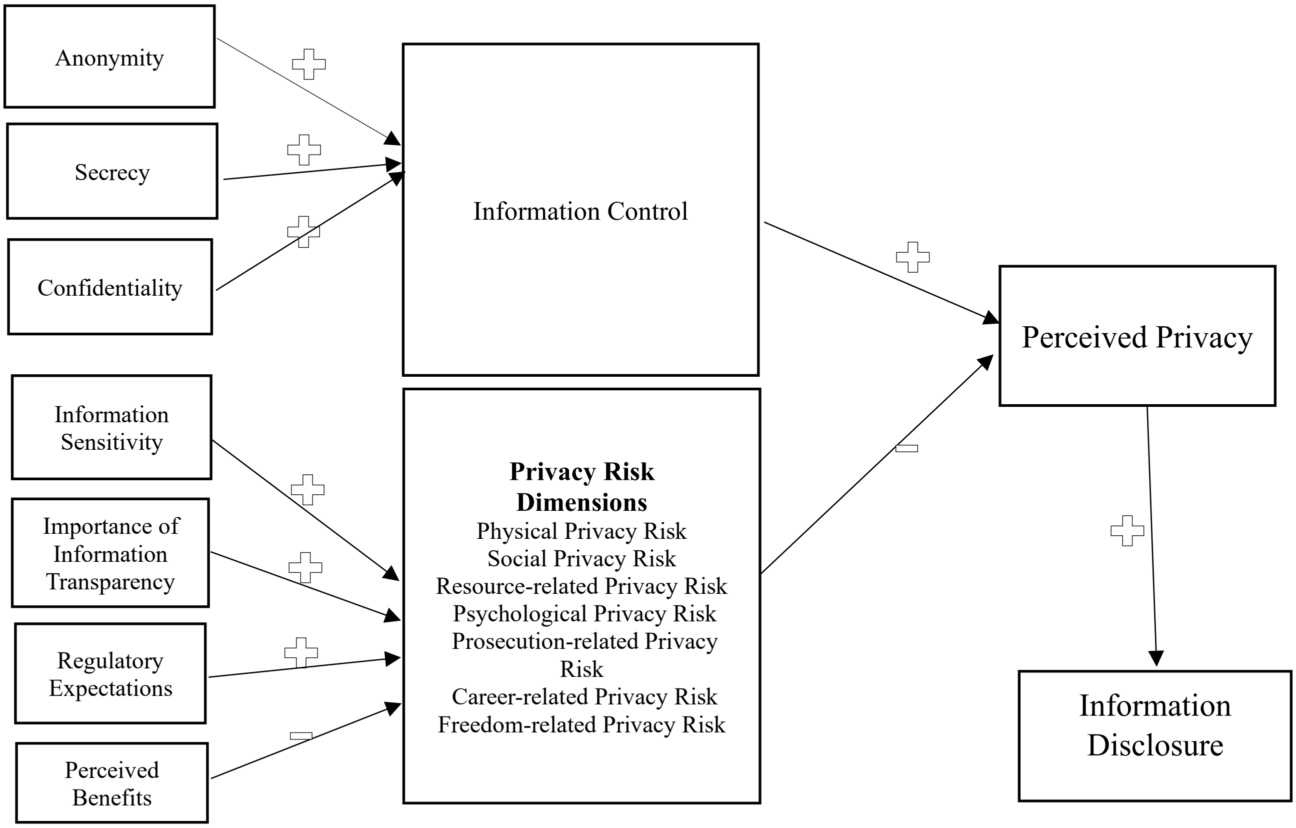
Anonymity
Secrecy
Confidentiality
Information Control
Information Sensitivity
Importance of Information Transparency
Regulatory Expectations
Perceived Benefits
Privacy Risk Dimensions
Physical Privacy Risk
Social Privacy Risk
Resource-related Privacy Risk
Psychological Privacy Risk
Prosecution-related Privacy Risk
Career-related Privacy Risk
Freedom-related Privacy Risk
Perceived Privacy
Information Disclosure
+
+
+
+
+
+
+
+
−
−

Figure 1. Privacy model

Table 1. Dimensions of privacy risk (Karwatzki et al., 2022)

Dimension	Definition The extent to which an individual believes that…	Example
Physical privacy risk	… a loss of physical safety may arise from access to his/her information	A woman believes that posting details (such as GPS tracking and lap times) about her every morning jog in the woods on a social media site could make her vulnerable to assault.
Social privacy risk	… a change in an individual's social status may arise from access to his/her information.	A teenager believes that sharing details on his favorite movies and leisure activities may lead to others bullying him.
Resource-related privacy risk	… a loss of resources may arise from access to his/her information.	A person believes that an insurance company might access her search history on Google to learn which diseases she has researched extensively in the past. She believes that they might assume that she has these diseases and then classify her accordingly in the insurance policy.
Psychological privacy risk	… a negative impact on his/her peace of mind may arise from access to his/her information.	An individual feels awkward about disclosing information about his daily life using instant messaging because he is afraid of surveillance and does not know what all this information could be used for in the future.
Prosecution-related privacy risk	… legal actions against him/her may arise from access to his/her information.	A man is afraid of identity theft when paying online with his credit card. He believes that his identity and payment information could be misused to access illegal content such as child pornography and that he may be held liable for that in the future.
Career-related privacy risk	… negative impacts on his/her career may arise from access to his/her information.	During her teenage years, a woman was in psychological treatment due to her bulimia and depression. She is afraid that her potential new employer may find out about this and consequently not hire her.
Freedom-related privacy risk	… a loss of freedom of opinion and be haviour may arise from access to his/her information.	An individual believes that entering a sensitive search term into a Web search engine may influence his chance to get a travel permit for a specific country.

Discussion and Implications

The proposed privacy model sheds light on dimensions of perceived privacy risks associated with using various devices and applications. As stated earlier, privacy risks impact privacy perception negatively. On the other hand, information control affects privacy perception positively. From the practical point of view, the proposed privacy model provides the industry with the factors that impact users perceived privacy and subsequent information disclosure and digital services use. Privacy perception may affect the use of various Internet connected apps and devices (Adrito, 2024; Magara & Zhou, 2024; Sicari et al., 2015). Offering information control by industry has a positive impact on privacy perception and may affect purchasing decisions. Therefore, the industry can use the proposed model to address perceived privacy, privacy risks, and user information control. Device manufacturers can also publish the privacy risk mitigation strategies and level of information control that is offered in their devices help users to make informed purchasing decisions. This model needs to be tested and validated in future research. The testing and validation of various factors that contribute to the users' privacy perceptions, according to this model, may be done by surveying users and analyzing their responses.

From the theoretical aspect, this research contributes to the topic of privacy by providing a privacy model, which can be built upon by including other factors that contribute to perceived privacy and information control. Other factors that contribute to perceived privacy and information control include culture, personality characteristics, and personal and institutional trust-related factors (Dinev et al., 2013; Xu, 2007; Bansal et al., 2010).

Limitations and Future Research

This study aimed to develop a privacy model that can be used to assess perceived privacy. As a result, factors that impact privacy perception were identified. There are other factors from prior research that have been identified to affect perceived privacy. These factors include context, culture, personality characteristics, and personal and institutional trust-related factors (Dinev et al. 2013). This study only addressed context. Additional factors may strengthen this model in future studies.

Future research may include other factors that affect perceived privacy. It is also important to develop metrics for privacy risks and privacy control. The proposed privacy model can be used to develop privacy metrics. Metrics for privacy risk and information control help to inform users about the privacy risks and privacy controls that are associated with a digital service and aid them in making informed decisions.

Conclusion

Internet connected devices such as IoT devices and smart home devices collect information and pose security and privacy risks. This study developed a privacy model based on prior research that can be used to assess perceived privacy based on privacy risk and control. The privacy model developed by this research is shown in Figure 1 and is composed of privacy controls and multidimensional privacy risks which affect privacy perception and information disclosure. Information control is attained by anonymity, secrecy, and confidentiality. Information control affects privacy perception positively.

Privacy risk consists of seven privacy-specific dimensions that include physical privacy risk, social privacy risk, resource-related privacy risk, psychological privacy risk, prosecution-related privacy risk, career-related privacy risk, and freedom-related privacy risk. Privacy risks are increased with information sensitivity, importance of information transparency, and regulatory expectations associated with information disclosure. However, perceived benefits of information disclosure decrease perceived privacy risks. The proposed privacy model can be used to develop privacy metrics. Metrics for privacy risk and information control provide users with a way to measure the privacy risks and privacy controls that are associated with digital services and assist them in making informed purchasing decisions. Future research will focus on developing privacy metrics based on the proposed model.

References

Ardito, L. (2024). Behavioural modeling for sustainability in smart home. *Proceedings of ARES 2024, Vienna*, 11 pages. https://doi.org/10.1145/3664476.3670946

Bansal, G., Zahedi, F. M., Grefen, D. (2010). The impact of personal dispositions on information sensitivity privacy concern and trust in disclosing health information online. *Decision Support Systems 49*(2), 138–150.

Bugeja, J., Jacobsson, A., &Davidsson, P. (2020). Is your home becoming a spy? A data-centered analysis and classification of smart connected home systems. *Proceedings of the 10th International Conference on the Internet of Things (IoT 2020), Malmo, Sweden*. ACM, New York, USA, 8 pages. https://doi.org/10.1145/3410992.3411012

Choi, D., Lowry, P. B., & Wang, G. A. (2020). The design of personal privacy and security risk scores for minimizing consumers' cognitive gaps in IoT settings. *Proceedings of the 53rd Hawaii International Conference on Systems Sciences.* 5076-5085. URL: https://hdl.handle.net/10125/64366 978-0-9981331-3-3

Dinev, T., Xu, H., Smith, H. J., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems, 22*(3), 295–316. https://doi.org/10.1057/ejis.2012.23

Haug, M., Lanza, J., & Gewald, H. (2021). Only if it affects me! The influence of privacy on different adoption phases. *Proceedings of the Forty-Second International Conference on Information Systems (ICIS 2021)*, Austin.10. 1-17.

Karwatzki, S., Trenz, M., & Veit, D. (2022). The multidimensional nature of privacy risks: Conceptualisation, measurement and implications for digital services. *Information Systems Journal, 32*, 1126-1157.

Lowry, P. B., Dinev, T., & Willison, R. (2017). Why security and privacy lies at the centre of the information Systems (IS) artefact: Proposing a bold research agenda. *European Journal of Information Systems, 26*(6), 546-563. DOI: 10.1057/s41303-017-0066-x

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

Protick, T. I., Sabir, A., Abhinaya, S., Bartlett, A., & Das, A. (2024). Unveiling users' security and privacy concerns regarding smart home IoT products from online reviews. *ACM J. Comput. Sustain. Soc. 2*(4), 44, 1-41. https://doi.org/10.1145/3685929

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trustin Internet of Things: The road ahead. *Computer Networks 76* (2015), 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1016.

Vemou, K., & Karyda, M. (2018). An evaluation framework for privacy impact assessment methods. *Proceedings of the Mediterranean Conference on Information Systems (MCIS 2018), 5*, 1-10.

Xu, H. (2007). The effects of self-construal and perceived control on privacy concerns. *Proceedings of the 28th Annual International Conference on Information Systems (ICIS)*. Montréal, Canada.