

DOI: https://doi.org/10.48009/2_iis_2026_105

Measuring privacy in smart homes: a multidimensional privacy metrics framework for IoT devices

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

Abstract

This study develops privacy metrics for smart home Internet of Things (IoT) devices through a synthesis of prior privacy and information systems research. Although smart home technologies provide benefits such as improved energy efficiency, convenience, security, and quality of life, the extensive collection and analysis of personal data by these devices raise significant privacy concerns that may hinder adoption. Prior studies have called for empirically measurable privacy frameworks and metrics for IoT and smart home environments. Building on the privacy metric model proposed by Etezady and Wang (2025), this research operationalizes privacy through formal quantification. Privacy is conceptualized as a perceived state influenced by perceived information control and perceived risk. Information control includes anonymity, secrecy, and confidentiality, while perceived risk encompasses physical, social, psychological, financial, and other multidimensional risks associated with information disclosure. Privacy metrics were developed through an extensive literature review and by adapting constructs from Dinev et al. (2013) and Karwatzki et al. (2022). The resulting framework consists of two sets of metrics: one for vendors to assess and improve device privacy, and another for measuring users' perceived privacy. The proposed metrics provide an empirically grounded approach for evaluating privacy in smart home environments.

Keywords: smart home IoT, privacy metrics, Internet of Things (IoT), perceived privacy, privacy risk, information privacy control

Introduction

The Internet of Things (IoT) refers to a large network of interacting physical objects such as vehicles, appliances, and thermostats with sensors and activators that are connected to the internet through data communication technology (Oberlander et al., 2018). These devices collect and exchange data through the Internet or other types of networks, although some users are not even aware of data collection, its scope, and its scale (Cichy et al., 2021). IoT enables objects to interact through their internet connection. IoT is changing businesses and enhancing lives. Applications of IoT include Smart Homes, Smart Healthcare, Industrial Automation, Smart Agriculture, Smart Transportation, Smart Environment, Smart Military, and Customer Asset Tracking (Magara & Zhou, 2024).

This paper focuses on smart home devices and the privacy issues associated with them. These devices collect enormous amounts of data, raising both privacy and security concerns that may hinder the adoption of smart home technologies. Smart home users need to be made aware of the volume of data collected and the associated privacy risks. Prior research has called for further studies to identify privacy metrics for IoT and smart home environments (Bugeja et al., 2020; Vemou & Karyda, 2018; Haug et al., 2021). This study

aims to develop privacy metrics for smart homes based on existing literature. The paper proceeds with a literature review, followed by the research approach and methodology. It then presents the proposed privacy metrics, and concludes with discussion and implications, study limitations, directions for future research, and a conclusion.

Background

Smart home devices are increasingly being utilized by consumers because they offer several benefits. Among the benefits are efficient use of energy and resources, improving quality of life, health benefits, and convenience (Magara & Zhou, 2024). Smart homes contribute to sustainability by leveraging technology to improve energy efficiency and optimize resource consumption. Interconnected devices and sensors accumulate data on users. Predictive analytics leverages machine learning algorithms and data mining techniques on collected data to anticipate users' needs and enable more efficient energy use (Ardito, 2024).

Smart homes by real-time monitoring and optimizing energy and resource consumption enhance energy efficiency. For example, smart thermostats through intelligent control systems that regulate settings based on the schedules and preferences of its users learn their routines and automatically adjust heating and cooling thereby saving energy at times when residents are not home. Smart lighting systems decrease energy usage by taking into account availability of natural lighting and occupancy. Smart water management systems, such as smart irrigation controllers, manage water usage efficiently by adjusting watering schedules based on data obtained from monitoring real-time weather conditions and moisture levels of soil. There are other examples of smart homes that contribute to health and well-being like air quality monitors that sense pollutants and allergens and activate air purifiers to maintain clean and safe air to breathe. There are also smart home security systems such as smart locks, motion detectors, and cameras that issue real-time alerts and provide remote monitoring enabling residents to monitor their homes remotely (Ardito, 2024).

The large amount of data that is collected on people through IoT devices endangers the security and privacy of people. Moreover, the vulnerabilities associated with IoT devices impact all users (Lowry et al., 2017; Protick et al., 2024). Concerns about online fraud, misuse of personal information, and no control over personal data cause mistrust and skepticism among consumers (Protick et al.).

Despite the benefits that smart home devices offer, there are privacy and security concerns because of the enormous amount of data that they collect, which can prevent adoption of smart home technologies. IoT devices can collect information about the device, its user, the device proximity to other devices, and use context. Analysis of the collected data can expose the behavior, preferences, and personality of users and possibly result in negative consequences for users (Cichy et al., 2021). In addition to transparency and strong privacy policies, strong security measures are also needed to address privacy concerns and establish user confidence and trust (Ardito, 2024; Magara & Zhou, 2024). Privacy issues arise from authorization issues, anonymization difficulties, data sharing, data retention, and user profiling issues. Addressing these issues requires a multifaceted approach including legislation, technology, user education, authorization, and security frameworks. Only by protecting individual privacy rights and lessening privacy risks can the potential of IoT be realized (Magara & Zhou, 2024).

The legacy definition of privacy is the right to be left alone (Warren & Brandeis, 1890). It is context-dependent and shaped by a dynamic interplay between individual needs and desires and those of society (Cinchy et al., 2021; Conger et al., 2013). Privacy is an abstract concept which is influenced by culture and jurisdiction. It has been created by humans as a result of legal, cultural, and organizational rules and policies

(Lowry et al., 2017). Privacy has to do with information that individuals want to keep private and is exchanged with desired goods and services such as online banking (Conger et al.). Privacy in most general terms has been regarded as a state and its empirically testable definition as ‘perceived (state of) privacy’ (Dinev et al., 2013). Researchers have also defined privacy as multidimensional, context dependent, elastic, and dynamic as it changes with life experiences (Dinev et al.; Karwatzki et al., 2022).

As Cinchy et al. (2021) noted, the users of IoT device are not made aware of precisely how much data is collected, integrated, and analyzed. To protect user privacy, several studies have called for more research on identifying privacy metrics with focus on IoT and smart homes (Bugeja et al., 2020; Vemou & Karyda, 2018; Haug et al., 2021). Other researchers have called for a clear, measurable, and empirically testable notion of privacy that can be used as a guide for legislation and privacy and security policies for government and organizations (Adrito, 2024; Dinev et al., 2013). A clear, measurable, and empirically testable privacy definition can be used by governments and organizations to develop management policies and practices that guard privacy and security of people (Dinev et al., 2013).

To empirically measure privacy, privacy related proxies including privacy concerns and privacy risks are used in research (Karwatzki et al., 2022; Smith et al., 2011). Privacy risk refers to the degree of one’s belief that negative outcome may result from known/unknown or authorized/unauthorized access to personal information. Users have privacy concerns over how their information is used by others. Privacy concerns are multidimensional and assist in understanding users’ perceptions of the behavior of data collectors (Karwatzki et al.). Privacy concerns can be defined as the concerns that users have from sharing information (Dinev & Hart, 2006; Warkentin et al., 2017).

Building upon the privacy metric model for IoT for home introduced by Etezady and Wang (2025), this paper seeks to operationalize that model through formal quantification. While the conceptual model provides a structural basis for privacy, it lacks a standardized measurement. To address this, we adapt the metrics originally proposed by Dinev et al. (2013) and Karwatzki et al. (2022) to enable evaluation of privacy in real-world scenarios. In essence, the prior conceptual model is translated into vendor-facing and user-facing metrics for smart home IoT devices.

Methodology

The evaluation in this study is based on the privacy metric model developed by Etezady and Wang (2025). In this model, privacy is conceptualized as a perceived state of privacy that influences information disclosure behavior. Perceived privacy is shaped by perceived information control and perceived risk. Perceived information control is influenced by anonymity, secrecy, and confidentiality. Factors affecting perceived risk include information sensitivity, the importance of information transparency, regulatory expectations, and perceived benefits. The model further characterizes perceived risk as multidimensional, encompassing physical, social, resource-related, psychological, prosecution-related, career-related, and freedom-related consequences. The privacy model used in this research is illustrated in Figure 1.

The privacy metrics for this research were developed by extensive examination of privacy literature from ACM, AIS, EBSCO, IEEE ejournals, ProQuest, Scopus, and Springer e-Journals using keywords such as IoT, privacy, and smart homes. This literature review identified the privacy measures developed by Dinev et al. (2013) and Karwatzki et al. (2022) as particularly relevant to the objectives of this study.

To measure perceived privacy, a set of metrics derived from Dinev et al. (2013) and Karwatzki et al. (2022) was employed. These measures were selected because they are consistent with the study's definition of

privacy and with the multidimensional nature of privacy risks incorporated into the proposed privacy metric model. Moreover, these measures have been previously validated in the aforementioned studies. To evaluate privacy control and privacy risks, the measures from Dinev et al. were adapted. To account for the different areas (privacy risk dimensions) that are impacted by information disclosure, the privacy risks construct of Karwatzki et al. were adapted.

The resulting Privacy metrics are shown in the appendix. The proposed privacy metrics in this study consist of two sets. The first set of metrics may be used by vendors to assess the level of privacy in their devices. The results of the vendors' privacy assessment may be used as a guide to enhance their products' privacy. The second set of metrics may be used to measure users perceived privacy of products. Privacy metrics for vendors are shown in tables A1 through A3 and for users in tables A4 through A6.

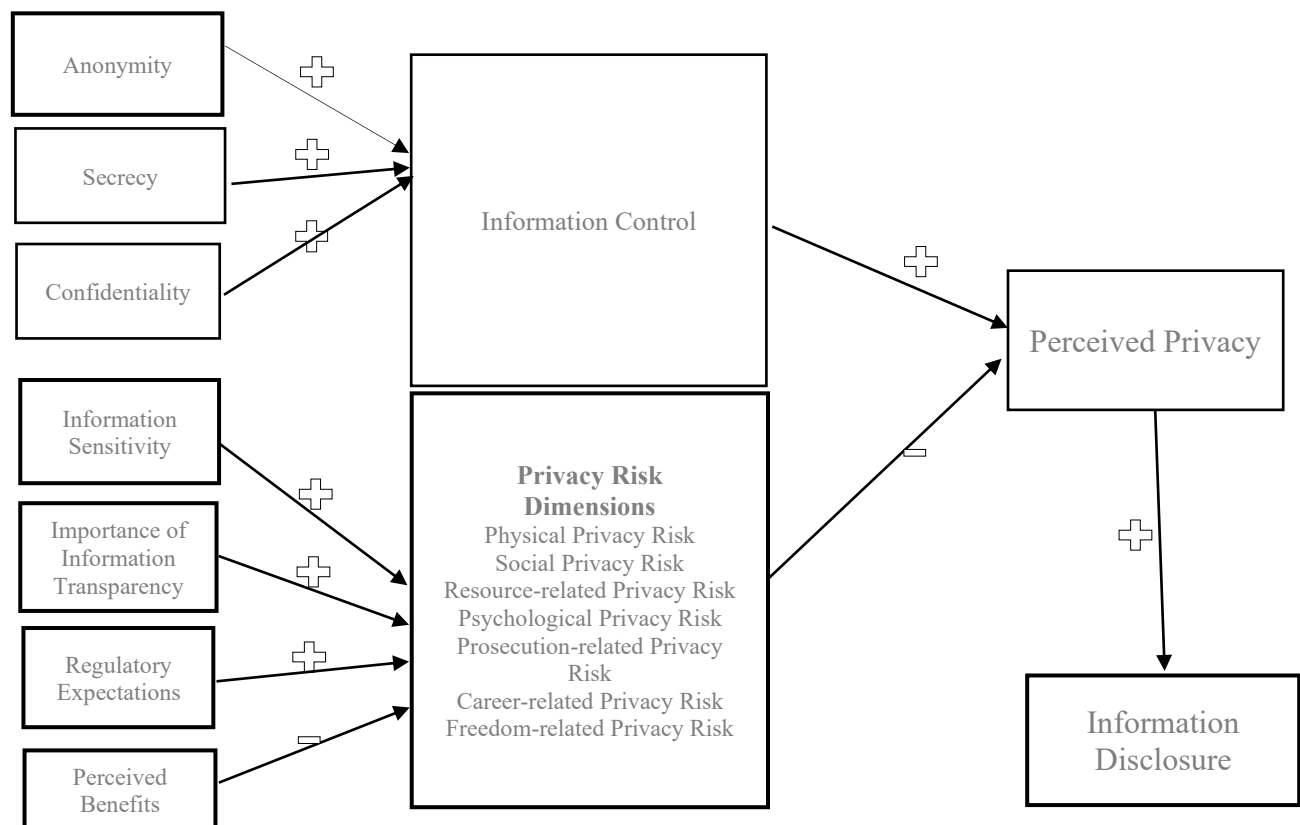


Figure 1: Privacy Model (Etezady & Wang, 2025)

Results and Discussion

This study developed privacy measures through a synthesis of prior research. These measures can be used by both consumers and businesses to evaluate product privacy. Businesses have a responsibility to protect consumer privacy, and device vendors may use the measurement instrument developed in this study to calculate a privacy score for their devices. In this process, responses to each questionnaire item can be assigned a score, and an overall privacy score can then be computed. The resulting score reflects the privacy level of a device, with higher scores indicating stronger privacy protections.

Potential buyers can compare the privacy scores of competing products, along with other criteria such as usability and device features, before making purchasing decisions. In addition, device manufacturers may use privacy scores to communicate and promote the privacy capabilities of their products for marketing purposes. Providing users with accessible privacy information and configurable privacy settings also contributes to consumer education and supports informed decision-making during the purchasing process. Privacy information should therefore be presented in a clear, simple, and understandable manner that requires minimal time and effort to review.

Consumers may also independently compute the privacy score of a smart device by completing the privacy measurement questionnaire. Vendors can facilitate this process by clearly disclosing the privacy features of their devices, thereby making it easier for users to evaluate privacy protections. By incorporating stronger data privacy features and providing transparent privacy information, device vendors can help reduce consumers' privacy concerns while enhancing the attractiveness of their products.

It should be noted that smart home devices vary significantly in functionality and design. Consequently, these privacy metrics should be tailored to the specific characteristics and requirements of different categories of smart home devices.

Implications for Research/Practice

All applications should be developed with privacy considerations integrated into their design. Privacy must be embedded into systems during the design and development phases rather than treated as an afterthought (Conger et al., 2013). Organizations can support a multifaceted approach to privacy protection by conducting Privacy Impact Assessments (PIAs). Similar to risk impact assessments, PIAs require organizations to evaluate their operations, personal data handling practices, and the associated privacy implications. This process helps identify potential privacy threats and implement appropriate controls to mitigate those risks. PIAs are typically conducted during the early stages of information system development. However, due to the rapid pace of technological change, not all privacy risks can be anticipated in advance. Consequently, privacy protection should be incorporated into the foundational architecture of systems rather than added after implementation (Oetzel & Spiekermann, 2014). As noted by Oetzel and Spiekermann, a PIA can be defined as "a risk assessment methodology used proactively in the design and upgrade phase of an IT system to make that system privacy friendly and compliant with data protection legislation." Accordingly, PIAs should be viewed as an ongoing process rather than a one-time compliance activity. They represent a continuous risk management approach involving standardized procedures for identifying, assessing, and mitigating privacy risks.

The privacy metrics developed in this research can serve as a framework for identifying the factors that should be considered in protecting user privacy. These metrics may be applied throughout the product development lifecycle to help ensure that appropriate privacy features and safeguards are incorporated into smart home IoT devices. In addition, the proposed metrics can provide guidance for the development of legislation, as well as organizational privacy and security policies and standards.

From a research perspective, this study represents one of the first efforts to develop comprehensive privacy metrics specifically for smart home IoT devices. The proposed framework can serve as a foundation for future studies aimed at extending and refining privacy metrics for a broader range of IoT applications and environments.

Limitations and Future Research

This research aimed to develop privacy metrics for smart home IoT devices based on the concept of perceived privacy, which is influenced by perceived information control and perceived risk. However, prior research suggests that perceived privacy is also shaped by additional factors, including culture, personality traits, and personal and institutional trust-related factors (Dinev et al., 2013). Incorporating measures for these additional variables could improve the comprehensiveness and effectiveness of privacy assessments for smart home products. Therefore, future research should explore the inclusion of other determinants of perceived privacy in the proposed framework. In addition, further studies are needed to validate and refine the proposed privacy metrics. Validation plans can include expert review, pilot testing with users, reliability analysis, factor analysis, convergent and discriminant validity testing, and comparison across different categories of smart home devices.

Conclusion

Smart home devices are increasingly adopted by consumers because of the many benefits they provide, including improved energy and resource efficiency, enhanced quality of life, health-related advantages, and greater convenience (Magara & Zhou, 2024). Despite these benefits, smart home devices collect vast amounts of user data, raising significant privacy and security concerns. As a result, users need to be aware of both the extent of data collection and the associated privacy risks.

A clear, measurable, and empirically testable definition of privacy can help users, governments, and organizations develop management policies and practices that better protect individuals' privacy and security (Dinev et al., 2013). To address this need, this research developed two sets of privacy metrics for smart home devices based on a synthesis of prior studies. These metrics are grounded in the privacy model proposed by Etezady and Wang (2025). While Etezady and Wang established the theoretical foundation of the model, the present study introduces the first set of standardized metrics derived from this framework. These metrics may serve as a reproducible benchmark for evaluating the privacy and security characteristics of smart home devices. The metrics developed in this study can assist vendors and users in assessing the privacy characteristics of smart home devices.

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>
- 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>
- Cichy, P., Salge, T. O., & Kohli, R. (2021). Privacy concerns and data sharing in the Internet of Things: Mixed methods evidence from connected cars. *MIS Quarterly*, 45(4), 1863-1892. [DOI:10.25300/MISQ/2021/14165](https://doi.org/10.25300/MISQ/2021/14165)
- Conger, S., Pratt, J. H., Loch, K. D. (2013). Personal information privacy and emerging technologies. *Information Systems Journal*, 23, 401-417. [doi:10.1111/j.1365-2575.2012.00402.x](https://doi.org/10.1111/j.1365-2575.2012.00402.x)

- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61-80.
- 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>
- Etezady, N., & Wang, P. (2025). A privacy metric model for IoT for homes (smart homes). *Issues of Information Systems*, 26(4), 17-24.
- 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](https://doi.org/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>
- Oberländer, A. M., Röglinger, M., Rosemann, M., & Kees, A. (2018). Conceptualizing business-to-thing interactions – A sociomaterial perspective on the Internet of Things, *European Journal of Information Systems*, 27(4), 486-502. [DOI: 10.1080/0960085X.2017.1387714](https://doi.org/10.1080/0960085X.2017.1387714)
- Oetzel, M. C., & Spiekermann, S. (2014). A systematic methodology for privacy impact assessments: a design science approach, *European Journal of Information Systems*, 23(2), 126-150, [DOI: 10.1057/ejis.2013.18](https://doi.org/10.1057/ejis.2013.18)
- 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>
- 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.
- Warkentin, M., Goel, S., & Menard, P. (2017). Shared benefits and information privacy: What determines smart meter technology adoption? *Journal of the Association for Information Systems*, 18(11), 758-786. [DOI: 10.17705/1jais.00474](https://doi.org/10.17705/1jais.00474).
- Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193-220.

Appendix of Privacy Metrics

The Likert-type scale employed to measure each privacy item should be defined separately for each device type.

Explanations for privacy items, where necessary, should be provided in the Privacy Enhancing Explanation column.

Table A1

Vendors Information Control Privacy Metrics

Metric Items	Likert-Type Scale	Privacy Enhancing Explanation
Anonymity		
Device users can hide their true identity when using this device.		
Device users can stay anonymous and fully use this device. If use is limited when anonymous explain the limitations.		
Device users' information can be kept anonymous, when using this device.		
Secrecy		
Users of this device can conceal some information, when they want to.		
Device users can falsify some of personal information if asked for by device.		
Users can refuse to give personal information to the device, when they think it is too personal.		
Confidentiality		
Personal information provided to the device remains confidential.		
Device vendor (manufacturer) prevents unauthorized people from accessing users' personal information in their databases.		
Users' personal information is only accessible to those authorized to have access.		

Table A2

Vendors Privacy Risk Metrics

Metric Items	Likert-Type Scale	Privacy Enhancing Explanation
Information Sensitivity		
List all the different type of information that is collected by the device.		
Perceived Benefits of Information Disclosure		
Device users need to reveal personal information to obtain		

information/products/services that they want. List the benefits users receive when they reveal personal information.		
Users need to provide personal information to use different features of the device.		
Device users need to disclose their personal information to benefit from a better, customized service and/or better information and products.		
Information Transparency		
Device users are informed what information about them is kept in the vendor's databases.		
Device vendor informs device users how long the collected information will be retained		
Device user is informed about the purpose for which user's information is collected.		
Regulatory expectations (LAW)		
There are laws that protect the users of the device from misuse of their personal data. List these law (s) if any.		
There are laws that govern and interpret the practice of how device vendor collects, uses, and protects device users' information. List these laws, if any.		
There are laws that address violation of the information that device users provide to device vendors. List these laws.		

Table A3

Vendors Privacy Risk Dimensions Metrics

Metric Items	Likert-Type Scale	Privacy Enhancing Explanation
If someone has access to the information this device collects...		
Physical Privacy Risk		
device user's physical safety might be impacted.		
device user might be exposed to physical threats.		
device user' chance of being physically harmed will be increased.		
it might endanger user's physical safety.		
Social Privacy Risk		

it might impact the perception that others have of the user.		
it might change the way people think about the user.		
user's social status might be influenced.		
user's peer group might think differently of the user.		
Resource-related privacy risk		
it might consume device user's time or money.		
it might cost device user time or money.		
it might require efforts or expenditures for the user.		
it might affect user's resources (e.g., time, money) negatively.		
Psychological privacy risk		
it might give device user a feeling of anxiety.		
it might cause inner restlessness for the device user.		
device user might experience mental tension.		
it might burden device user mentally.		
Prosecution-related privacy risk		
device user might become judicially indictable, either wrongly or rightfully.		
device user might be prosecuted due to wrongful or rightful suspicions.		
device user might be held legally accountable due to incorrect or correct suspicions.		
device user might be held responsible due to incorrect or correct suspicions.		
Career-related privacy risks		
it might reduce device user's career prospects.		
it might affect device user's career negatively.		
it might make it difficult for the device user to be successful in his/her job.		
it might result in a negative shift in the device user's career.		
Freedom-related privacy risk		
device user's opinions or behavior might be manipulated.		
device user's thoughts or actions might be influenced externally.		

device user's mindset or device user's resulting behavior might be influenced.		
device user's attitude or behavior might be influenced.		

Table A4

Users Information Control Privacy Metrics

Metric Items	Likert-Type Scale	Privacy Enhancing Explanation
Anonymity		
I believe I can hide my true identity when using this device.		
I believe I can stay anonymous and do everything I want on this device.		
I can keep my information anonymous, when using this device.		
Secrecy		
I believe I can conceal some information from this device when I want to.		
I feel I can falsify some of my personal information if it is asked for by this device.		
I believe I can refuse to give my personal information to this device, when I think it is too personal.		
Confidentiality		
I believe my personal information provided to this device remains confidential.		
I believe the device vendor (manufacturer) prevents unauthorized people from accessing my personal information in their databases.		
I believe my personal information is only accessible to those authorized to have access.		

Table A5

Users Privacy Risk Metrics

Metric Items	Likert-Type Scale	Privacy Enhancing Explanation
Information Sensitivity		
When using smart devices that collect information, many people find there is some information that they generally feel comfortable providing, some information they feel comfortable providing only under certain conditions, and some information is too personal that they never or rarely feel comfortable providing. Please indicate how much you agree with the following statements:		

I do not feel comfortable with the type of information this device requests from me.		
I feel that this device gathers highly personal information about me.		
The information I provide to this device is very sensitive to me.		
Perceived Benefits of Information Disclosure		
Revealing my personal information on this device will help me obtain information/products/services I want.		
I need to provide my personal information so I can get exactly what I want from this device.		
I believe that as a result of my personal information disclosure, I will benefit from a better, customized service and/or better information and products.		
Information Transparency		
Device vendor allows me to find out what information about me is kept in their databases.		
The device vendor informs me how long they will retain information they collect from me.		
Device vendor informs me about the purpose for which this device wants to collect information from me.		
Regulatory expectations (LAW)		
There are laws that protect me from misuse of my personal data by smart device vendors.		
There are laws that govern and interpret the practice of how device vendor collects, uses, and protects my information.		
There are laws that address violation of the information that I provide to device vendors.		

Table A6

Users Privacy Risk Dimension Metrics

Metric Items	Likert-Type Scale	Privacy Enhancing Explanation
If someone has access to the information this device collects...		
Physical Privacy Risk		
my physical safety might be impacted.		

I might be exposed to physical threats.		
the chance of me being physically harmed will be increased.		
it might endanger my physical safety.		
Social Privacy Risk		
it might impact the perception that others have of me.		
it might change the way people think about me.		
my social status might be influenced.		
my peer group might think differently of me.		
Resource-related privacy risk		
it might consume my time or my money.		
it might cost me time or money.		
it might require efforts or expenditures.		
it might affect my resources (e.g., time, money) negatively.		
Psychological privacy risk		
it might give me a feeling of anxiety.		
it might cause inner restlessness.		
I might experience mental tension.		
it might burden me mentally.		
Prosecution-related privacy risk		
I might become judicially indictable, either wrongly or rightfully.		
I might be prosecuted due to wrongful or rightful suspicions.		
I might be held legally accountable due to incorrect or correct suspicions.		
I might be held responsible due to incorrect or correct suspicions.		
Career-related privacy risks		
it might reduce my career prospects.		
it might affect my career negatively.		
it might make it difficult to be successful in my job.		
it might result in a negative shift in my career.		
Freedom-related privacy risk		
my opinions or behavior might be manipulated.		
my thoughts or actions might be influenced externally.		

my mindset or my resulting behavior might be influenced.		
my attitude or behavior might be influenced.		