Vision: Why Johnny Can't Configure Smart Home? A Behavioural Framework for Smart Home Privacy Configuration

Joseph Shams
Department of Informatics
King's College London
London, UK
joseph.shams@kcl.ac.uk

Nalin A. G. Arachchilage
Optus La Trobe Cyber Security Research Hub
Department of Computer Science and IT
La Trobe University, Australia
nalin.asanka@latrobe.edu.au

Jose M. Such
Department of Informatics
King's College London
London, UK
jose.such@kcl.ac.uk

Abstract—**Despite the advancements in smart technologies, the lack of user awareness of the capabilities of IoT smart home devices can expose them to privacy breaches. For example, a user may be unaware that their smart home devices are recording and storing their conversations (e.g. personal, perhaps sensitive or confidential communications). It could be argued that this is due to the lack of users' threat perceptions and the challenges of altering existing (smart home) configuration behaviours. Therefore, we propose a behavioural framework to enhance users' smart home configuration behaviours through their motivation. To develop the framework, we derived and extended the elements from the Technology Threat Avoidance Theory (TTAT) and Fogg's Behavioural Motivation (FBM) model. The elements of the proposed framework were incorporated into an application scenario, i.e. a game design. The designed gaming application aims to educate users about smart home device capabilities and enhance their configuration behaviour through motivation. More research is required to evaluate the proposed framework and its gaming application scenario through empirical investigations.**

Index Terms—**Usable security, IoT smart homes, Privacy, User centred design, Serious games**

1. Introduction

When configuring IoT smart home devices, an obstacle is presented in the form of inadequately designed configuration tools and interfaces [10, 12, 17, 26] that offer minimal education to the user. These configuration tools, a form of a safeguard measure, may not cater to all technical abilities, where users are expected to self-educate and configure their devices independent from any advice from the configuration tool [35]. Furthering this problem, the technology that smart devices are built on is foreign to many users who prioritise the convenience a device functionality offers over their privacy [34]

A study found various cases where smart cameras were broadcasting sensitive data including geographical locations and sometimes username and password combinations [10]. These capabilities require configuring to reflect users' privacy preferences. The configuration of each capability is time-consuming and complicated [26] for non-technical users and is amplified by each additional smart device installed. In other cases, users simply do not know how to protect themselves [1, 3, 14, 25]. Another privacy breach caused by the lack of smart device configuration includes a family from Leeds who had their smart camera feeds accessed thousands of times by unauthorised parties, made available via the remote control feature [8]. This occurred after the owners installed and setup their smart camera without any knowledge or consent provisions.

This lack of awareness illustrates a need for the redesign of smart home configuration tools and their interfaces by understanding users' *threat perception* and users' psychological behaviours when configuring smart home devices [1, 10, 13, 26, 34]. Instances of inadequate tools and educational interfaces include users accepting and integrating the current recommended data practices for smart devices. Users are even less likely to engage with new safeguard measures, such as the Personalised Privacy Assistant (PPA) for IoT [15] and Databox [27], as this would require more effort on their part [13], consequently resigning to the lack of privacy protection offered to them. These safeguard measures do not offer useful and actionable information that can motivate users to acknowledge smart device capabilities, alongside privacy implications [13]. Therefore, it is still an open question how to motivate smart home configuration behaviours to overcome users feeling resigned to using safeguard measures that may not offer the level of control and the level of protection they desire [13].

The absence of motivation towards better configuration behaviours results in users being unaware of the privacy implications of potential data leakage, inferable data and unauthorised access to other personally identifiable information [15, 16, 18]. Example implications of smart device capabilities include 24 hours surveillance by smart cameras [28] and smart lights offering adversaries entry points into the smart home network, making it possible to disable a smart alarm if installed [20]. It can be argued that motivation can be enhanced if users perceived these threats [7].

To enhance smart home configuration behaviours and raise awareness of smart device implications, users require more motivation to appropriately assess and act upon smart device capabilities. A tool that has been successful in changing users' existing behaviours is game-based learning approaches [6, 7]. While game-based learning has been successful in changing existing behaviours, its use for raising user awareness smart home environments is often overlooked.

Gamification can provide a better learning environment than traditional book learning techniques [2] by enhancing motivation while retaining the players' attention through engaging aims and objectives [2, 7] presented as a story. Traditional learning approaches are time-consuming and cognitively exhaustive, which negatively impact on motivation. Whereas, gamification can provide an environment that contains a limited about of functionality with engaging goals and objectives to motivate and retain player attention. This can motivate users to transition towards different mental states where they are ready to learn new concepts in a comfortable environment [5]. For example, an educational game may motivate PPA and Databox users to discover and configure settings that they were not aware of, to begin with. This may encourage users to search and unearth more configuration setting they did not know exist.

As the current literature regarding smart home configuration indicates that *threat perceptions* and the steps individuals can take to protect their privacy need advancing, gamification can be a useful tool to enhance intrinsic motivation within users during smart home configuration. For example, if control mechanisms, such as PPA for IoT and Databox, gamified the smart home configuration process to create a learning environment alongside implementing persuasive design techniques, users may be intrinsically motivated to protect their privacy. Intrinsic motivation refers to the completion of tasks due to the inherent satisfaction of performing the task and the willingness of users to invest more cognitive and physical effort into a task [9].

The noteworthy contribution of this paper is a behavioural framework designed as an educational intervention for enhancing people's smart home device configuration behaviours. In section, 2 the framework designed to enhance smart home configuration behaviours is detailed. Following this, an example application scenario is provided in section 3 to demonstrate how this framework can be implemented in a working environment (i.e. an application scenario). This paper concludes by stating the next steps that are required to examine the proposed framework and its gaming application scenario through empirical investigations.

2. A Framework for Smart Home Configuration

The proposed framework aims to enhance people's smart home configuration behaviour through their motivation by deriving and extending elements from TTAT [23] and Fogg's Behavioural Motivation (FBM) model [19].

TTAT explains individual IT users' behaviour of avoiding malicious IT threats such as phishing attacks (Figure 1) [23] [7]. Furthermore, the model describes how one can avoid malicious IT threats (in our case privacy threats such as data breaches or data leaks) by using a given safeguard measure. The safeguard measure does not have to be technology-based such as privacy-preserving tools, for example (Tor [25]) and can include a user's smart home configuration behaviour.

Consistent with TTAT [23], people's IT threat avoidance behaviour is determined by their avoidance motivation, which, in turn, is affected by perceived threat. Perceived threat is influenced by perceived severity and susceptibility. Perceived threat is also influenced by the interaction of perceived severity and susceptibility. People's avoidance motivation is also determined by three constructs; safeguard effectiveness, safeguard cost and self-efficacy. Therefore, the hypotheses (H) developed from TTAT [23] are described in the context of individuals' smart home configuration behaviour as follows:

H1. Motivation (derived from TTAT) positively affects individual's smart home configuration behaviour.

H2. Perceived "privacy" threat positively affects individual's motivation.

H3a. Perceived severity positively affects individual's perceived "privacy" threat.

H3b. Perceived susceptibility positively affects individual's perceived "privacy" threat.

H3c. The combination of perceived severity and perceived susceptibility positively affects individual's perceived "privacy" threat.

H4. Safeguard effectiveness positively affects individual's motivation to configure their smart home devices.

H5. Safeguard cost negatively affects individual's motivation to configure their smart home devices.

H6. Self-efficacy positively affects individual's motivation to configure their smart home devices.

Whilst the TTAT [23] forms behavioural elements that need to be incorporated into the framework for enhancing individuals' smart home configuration behaviour, it also helps in the identification of interface (i.e. PPA or Databox) design elements that can promote better user interaction and appropriate trust decisions for preserving privacy. Persuasive Design (PD) technology is used in this research to change individuals' behaviours through persuasion and social influence [33]. Accordingly, *ability*, *prompt* and *motivation*, elements derived and extended from the Fogg's Behavioural Motivation (FBM) model [19] are used in the framework to enhance individuals' behaviour towards smart home configuration.

Consider, for example, developing *privacy nudges* for PPA or Databox to enhance individuals' smart home configuration behaviour [24]. Previous research has revealed that privacy nudges increase awareness of apps' behaviours and *motivate* users to review and adjust their app permissions [3]. It also *motivates* them to revisit their earlier decisions [24]. Therefore, *privacy nudges* can be designed as a means to motivate individuals' *ability* to interact with permission settings of PPA or Databox. Privacy nudging features of PPA for IoT or Databox, like many other features, persuades individuals to take actions. The goal of this exercise is that individuals will have sufficient motivation and ability through the interface (of PPA or Databox) to adopt an appropriate privacy-preserving behaviour. This approach helps to explain the hypotheses (H) developed from Fogg's Behavioural Model (PBM) [19] which is described in the context of individuals' smart home configuration behaviour as:

H7. Motivation (derived from PD: Fogg's Behavioural Model) positively affects individual's smart home configuration behaviour.

H8. Ability positively affects individual's smart home configuration behaviour.

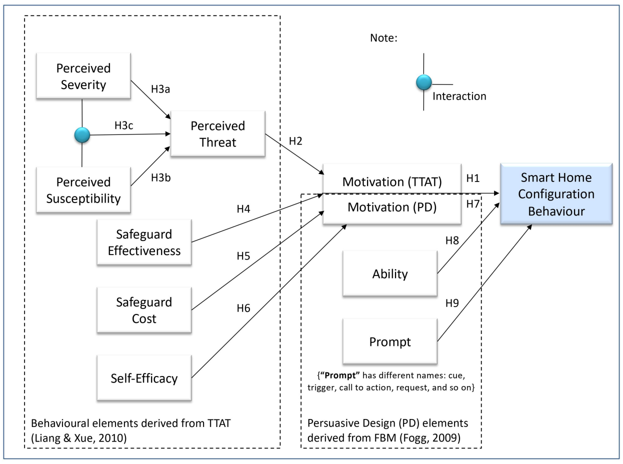
Note:
Interaction
Perceived Severity
H3a
Perceived Threat
H3c
H2
Perceived Susceptibility
H3b
Motivation (TTAT)
H1
Smart Home Configuration Behaviour
Motivation (PD)
H7
H4
Safeguard Effectiveness
H5
H8
Ability
Safeguard Cost
H6
H9
Prompt
("Prompt" has different names: cue, trigger, call to action, request, and so on)
Self-Efficacy
Behavioural elements derived from TTAT (Liang & Xue, 2010)
Persuasive Design (PD) elements derived from FBM (Fogg, 2009)

Figure 1. A behavioural framework for the Smart Home Configuration (elements derived and extended from TTAT [23] and FBM [19])

H9. Prompt (i.e. Trigger) positively affects individual's smart home configuration behaviour.

Another example is, applying the developed framework (Figure 1), into a game design scenario as a means of an educational intervention that can enhance the people's smart home configuration behaviour.

3. Application Scenario

The primary aim of the game design application scenario established by this paper is to provide educational interventions to enhance users' smart home configuration behaviours. As users interact with the game, their understanding of smart device capabilities will be developed. This will enrich users' *threat perceptions* and increases *self-efficacy* by remodelling users' psychological evaluation of their smart device configuration behaviours.

Gamification can encourage intrinsic motivation, demonstrating how successful the educational tool has been in engaging with users [14]. Intrinsic motivation refers to the completion of tasks due to the inherent satisfaction of performing the task and the willingness of users to invest more effort into a task [9].

3.1. What to teach

Figure 2 shows the available smart devices in the game. Players are expected to install four out of the seven devices drawn on the board. The objective of the game is to help and encourage a player to install the minimum number of smart devices that can, in total, offer the maximum number of smart *capabilities* while minimising the risk and exposure to privacy threats. It is important to re-emphasise that while a player is presented with *smart devices*, the objective is to install *smart capabilities*. For example, a security camera and a smart TV may both offer visual monitoring of the inside of the player's smart home. In this case, while reviewing the options the player is informed of the extent and limitations, as well as the associated risk, of each device's capabilities in monitoring before making privacy decisions.

There are a limited number of approaches for configuring IoT smart home devices, with fewer educational tools to guide users through the configuration process[21]. One such approach involves employing control mechanisms that offer interfaces with which users can interact with their devices [11]. Another would include the behavioural choices users make [5].

Previous research has identified users' feeling of resignation in terms of the inadequate privacy controls over their smart home devices [13], as well as the need for the re-education of smart home users on the breadth of device capabilities [21], allowing users to assess these devices and make informed decisions.

The game design should develop users' *ability* to identify device capabilities (*threat perception*), whilst simultaneously *motivating* changes in configuration behaviours (*self-efficacy*) with *prompts*. Examples of these capabilities include delegation, remote control and connectedness. [22, 29, 31, 32, 35]. The ordering of smart devices by severity is based on the results of a set of interviews conducted by Seymour et al., [32] looking to uncover participants' threat perceptions of different smart device capabilities and their feelings on those capabilities, those mentioned below.

The list below demonstrates the capabilities ordered from least severe to most severe must be examined. To identify this correct ordering, the severity of each capability and the extent to which data collections can occur, and the granularity of the collections. For example, a smart camera can perform a range of capabilities such as *Sensing* in the form of video and audio surveillance, connectedness to the internet and the ability to remote control and stream video feeds to accompanying applications [10, 32].

1) **Connectedness:** The ability for smart devices to connect to the internet,
2) **Delegation:** Automate tasks on the user's behalf,
3) **Learning/Sensing:** Learn from past interactions to alter device behaviour,
4) **Voice Control:** Voice-activated commands spoken that allow the user to interact with their device,
5) **Remote Control:** Allows remote control and monitoring of smart devices via an external application

For this example, *Connectedness* can be rated 1/5 as it is a fundamental requirement for smart devices to perform "smart" features; *Delegation* can be rated 2/5 as users have expressed the least reservations for its use and *sensing* can be rated 5/5 as it can compromise the privacy of everyone within the smart environment [32]. To create a list of capabilities that can capture the range that truly exists, this game uses the definition of "smartness", as presented by Seymour et al., [32], to label the actions smart devices can perform.

By educating smart home users on various device capabilities and the level of privacy exposure their use can incur, users can begin to acknowledge their part in protecting their privacy (*safeguard effectiveness*). Also, the cognitive and physical efforts (*safeguard costs*) required by users to configure their devices can be lessened therefore limiting how often users are overwhelmed by the number of decisions that need to be made, current problem users face [26].

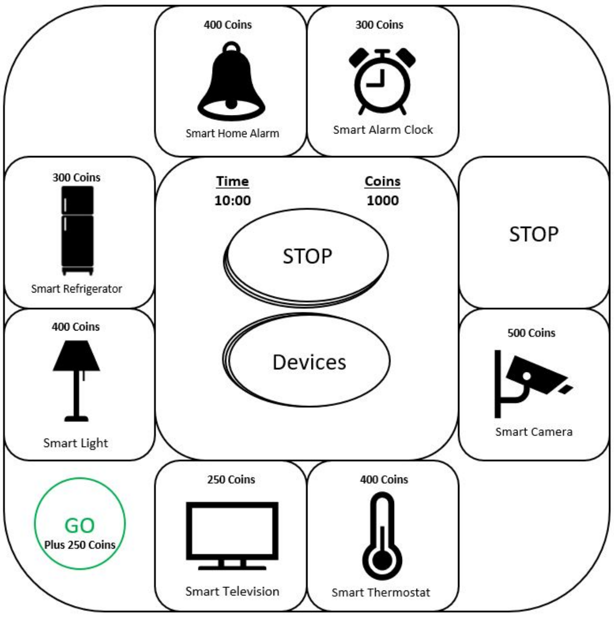

Figure 2. Behavioural framework application scenario for enhancing smart home configuration behaviours

3.2. Story

An example story, shown in figure 2, targeting the elements of the behavioural framework presented in section 2 is described below. The story presents a learning environment where the player is encouraged to critically analyse smart device capabilities, demonstrating their *threat perceptions*. Furthermore, by enhancing *threat perceptions* and through the use of *prompts*, *safeguard effectiveness* can be improved through learning the different actions they can take to limit device capabilities. *Prompts* are presented to users highlighting implications of smart device capabilities. By educating players on the capabilities of smart devices, the process of determining the severity of privacy risks associated with smart devices can be simplified, increasing the *ability* of the players.

The amount of cognitive and physical effort required by users will begin to reduce when players become familiarised with device capabilities, lowering the *safeguard costs* that users incur. By enhancing *threat perceptions*, in a learning environment while also attempting to reduce cognitive and physical efforts when configuring smart homes, should raise user confidence of how much power they have over their own devices, demonstrating *self-efficacy*. The player begins on the “Go” field. The “Go” field indicated the starting position and the start of a new round. The player rolls a dice and moves their piece according to the number thrown. The ”Stop” tile attempts to prove users with additional information, informing them of what practical steps they can take themselves to protect their privacy.

3.3. Game design Principles

The story mentioned in section 3.2 shall incorporate a set of guidelines recommended for designing educational games [4, 5, 30]. These game design principals describe how the user interacts with the game. Prensky [30] has proposed that games can be described in terms of six architectural elements. Those elements were used as guidelines for structuring and presenting the information in the game in section 3.2.

Rules. The rules are designed to organise the game to maximise the educational aspects. The story is developed based on the framework presented in section 2, derived from the TTAT and FBM.

Goals and objectives. The goals and objectives of the game are to encourage players to install the minimum number of smart devices that can, in total, offer the maximum number of smart capabilities while minimising the risk and exposure to privacy threats. This is accomplished within the available time. It is important to re-emphasise that while a player is presented with smart devices, the goal is to install smart capabilities. By completing this game, the player will be more aware of the different capabilities IoT smart home devices can perform, and the severity of these capabilities, enhancing their threat perception. These goals and objectives provide players with simulating tasks that attempt to promote intrinsic motivation, increasing the effectiveness of educational tools.

Outcome and feedback. This allows for the players’ progress to be measures against the goals and objectives, targeting their *ability*. Players receive real-time feedback when decision making in the game. For example, when players are ordering smart device capabilities, they are presented with a green tick or a red cross, demonstrating whether the decisions users have made are correct. Further feedback is presented to the player through *prompts* that aim to surface the risks of smart device capabilities, *motivating* users to take action and restrict capabilities. For example, users may be presented with the following statement, “The more you use smart devices, the more dependant you may become on third party assistance!” or “Smart devices may be capable of monitoring privacy activities without your consent!”.

Players excitement and engagement. To sufficiently keep player’ engagement, the opportunity to earn points, and risks of losing points, when ordering device capabilities and purchasing smart devices is introduced into the application scenario. For example, each smart device has a cost that reflects the risks and the costs of the device. For example, always-on monitoring cameras (such as security cameras) will cost more than an on-demand camera (such as smart TVs) from 50 to 100 coins each.

Human computer interaction. This is achieved by providing timely, actionable feedback coupled with a points system. An example of timely feedback would be during the ordering phase. When players are ordering capabilities by severity, a red cross will remain next to the box, as shown by figure 3, until the player enters the capability into the correct order.

Representation or story. For educational purposes, real-world interactions and aspects of reality are exaggerated. The story is presented as a board game where the player progresses through the game, making their way around the board.

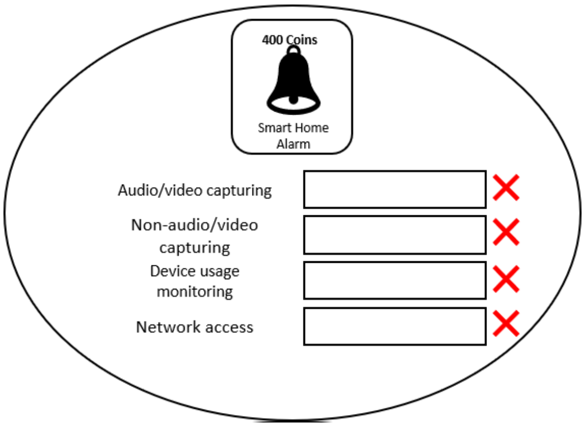

Figure 3. Example device card from application scenario for enhancing smart home configuration behaviours

4. Future work and open challenges

This research presents a framework for enhancing smart home configuration behaviours through building motivation. This framework was then applied to a possible game design scenario (Figure 1). Several evaluations are required, these include:

1) Evaluation of the framework developed in section 2. Further research is required to evaluate the proposed framework and its gaming application scenario through empirical investigations. This will take the form of a scenario-based or participatory-based storyboarding design.
2) Evaluation of game prototype in section 3 addressing the elements of the framework in section 2. A think-aloud protocol can be employed on the developed gaming prototype (i.e. low or high fidelity board game prototype). Players (i.e. users) are asked to interact with the developed board game along with the pre and post-study tests. Finally, think-aloud data along with the pre and post-study can be used to evaluate players' behavioural impact on the developed framework 2 when configuring smart home device capabilities.

5. Conclusion

The main contribution reported in this paper is the creation of a behavioural framework that enhances users' smart home configuration behaviours through the application of behavioural and motivation models [19, 23]. To develop the framework, we derived and extended elements from Technology Threat Avoidance Theory (TTAT) [23] and Fogg's Behavioural Motivation (FBM) model [19]. This behavioural framework has been incorporated into a possible application scenario, in our case a board game application design [19].

The application scenario introduces an environment where players are asked to review the capabilities of smart devices while being presented with actionable and useful prompts that aim to develop users' threat perceptions alongside strengthening users' motivation towards protecting their privacy from the threats introduced by smart home devices. At present, the application scenario (i.e. game prototype application) is under development, intending to produce a proof of concept solution that can be empirically evaluated through a scenario or participatory-based study. The evaluation of the application scenario can begin to detail the success of the framework and application scenario in updating smart home users' perceptions of smart device capabilities to allow for more informed decision making. With this, further attempts to provide educational interventions for enhancing human behavioural models for smart home configuration behaviours can be investigated.

References

[1] Noura Abdi, Kopo M Ramokapane, and Jose M Such. More than smart speakers: security and privacy perceptions of smart home personal assistants. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS)*, 2019.

[2] Adnan Ahmad, Furkh Zeshan, Muhammad Salman Khan, Rutab Marriam, Amjad Ali, and Alia Samreen. The impact of gamification on learning outcomes of computer science majors. *ACM Transactions on Computing Education (TOCE)*, 20(2):1–25, 2020.

[3] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. Your location has been shared 5,398 times! a field study on mobile app privacy nudging. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, pages 787–796, 2015.

[4] Alan Amory and Robert Seagram. Educational game models: conceptualization and evaluation: the practice of higher education. *South African Journal of Higher Education*, 17(2):206–217, 2003.

[5] Nalin Asanka Gamagedara Arachchilage and Melissa Cole. Design a mobile game for home computer users to prevent from "phishing attacks". In *International Conference on Information Society (i-Society 2011)*, pages 485–489. IEEE, 2011.

[6] Nalin Asanka Gamagedara Arachchilage and Steve Love. A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, 29(3):706–714, 2013.

[7] Nalin Asanka Gamagedara Arachchilage, Steve Love, and Konstantin Beznosov. Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, 60:185–197, 2016.

[8] BBC. Smart camera and baby monitor warning given by uk's cyber-defender, 2020.

[9] Max V Birk, Cheralyn Atkins, Jason T Bowey, and Regan L Mandryk. Fostering intrinsic motivation through avatar identification in digital games. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 2982–2995, 2016.

[10] Joseph Bugeja, Désirée Jönsson, and Andreas Jacobsson. An investigation of vulnerabilities in smart connected cameras. In *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 537–542. IEEE, 2018.

[11] George Chalhoub. The ux of things: Exploring ux principles to inform security and privacy design in the smart home. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems Extended Abstracts*, pages 1–6, 2020.

[12] Pierre Ciholas, Aidan Lennie, Parvin Sadigova, and Jose M Such. The security of smart buildings: a systematic literature review. *arXiv preprint arXiv:1901.05837*, 2019.

[13] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. Informing the design of a personalized privacy assistant for the internet of things. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2020.

[14] Edward Curry, Willem Fabritius, Souleiman Hasan, Christos Kouroupetroglou, Umair ul Hassan, and Wassim Derguech. A model for internet of things enhanced user experience in smart environments. In *Real-time Linked Dataspaces*, pages 271–294. Springer, 2020.

[15] Anupam Das, Martin Degeling, Daniel Smullen, and Norman Sadeh. Personalized privacy assistants for the Internet of Things: Providing users with notice and choice. *IEEE Pervasive Computing*, 17(3):35–46, 2018.

[16] Sofia Dutta, Sai Sree Laya Chukkapalli, Madhura Sulgekar, Swathi Krithivasan, Prajit Kumar Das, Anupam Joshi, et al. Context sensitive access control in smart home environments. In *6th IEEE International Conference on Big Data Security on Cloud (BigDataSecurity 2020)*, 2020.

[17] Jide S Edu, Jose M Such, and Guillermo Suarez-Tangil. Smart home personal assistants: A security and privacy review. *arXiv preprint arXiv:1903.05593*, 2019.

[18] Earlence Fernandes, Jaeyeon Jung, and Atul Prakash. Security analysis of emerging smart home applications. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 636–654. IEEE, 2016.

[19] Brian J Fogg. A behavior model for persuasive design. In *Proceedings of the 4th international Conference on Persuasive Technology*, pages 1–7, 2009.

[20] JC Hu. How one lightbulb could allow hackers to burgle your home. quartz, 2018.

[21] Yue Huang, Borke Obada-Obieh, and Konstantin Beznosov. Amazon vs. my brother: How users of shared smart speakers perceive and cope with privacy risks. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2020.

[22] Andreas Jacobsson, Martin Boldt, and Bengt Carlsson. A risk analysis of a smart home automation system. *Future Generation Computer Systems*, 56:719–733, 2016.

[23] Huigang Liang and Yajiong Xue. Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7):394–413, 2010.

[24] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, S Aerin Zhang, Norman Sadeh, Y Agarwal, and A Acquisti. Follow my recommendations: A personalized privacy assistant for mobile app permissions. In *Symposium on Usable Privacy and Security*, 2016.

[25] Akshaya Mani, T Wilson-Brown, Rob Jansen, Aaron Johnson, and Micah Sherr. Understanding tor usage with privacy-preserving measurement. In *Proceedings of the Internet Measurement Conference 2018*, pages 175–187, 2018.

[26] Karola Marky, Verena Zimmermann, Alina Stöver, Philipp Hoffmann, Kai Kunze, and Max Mühlhäuser. All in one! user perceptions on centralized iot privacy settings. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems Extended Abstracts*, pages 1–8, 2020.

[27] Charith Perera, Susan YL Wakenshaw, Tim Baarslag, Hamed Haddadi, Arosha K Bandara, Richard Mortier, Andy Crabtree, Irene CL Ng, Derek McAuley, and Jon Crowcroft. Valorising the iot databox: creating value for everyone. *Transactions on Emerging Telecommunications Technologies*, 28(1):e3125, 2017.

[28] James Pierce. Smart home security cameras and shifting lines of creepiness: A design-led inquiry. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2019.

[29] James Pierce, Richmond Y Wong, and Nick Merrill. Sensor illumination: Exploring design qualities and ethical implications of smart cameras and image/video analytics. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–19, 2020.

[30] Marc Prensky. Digital game-based learning. *Computers in Entertainment (CIE)*, 1(1):21–21, 2003.

[31] Evgenia Princi and Nicole Krämer. I spy with my little sensor eye-effect of data-tracking and convenience on the intention to use smart technology. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2020.

[32] William Seymour, Reuben Binns, Petr Slovak, Max Van Kleek, and Nigel Shadbolt. Strangers in the room: Unpacking perceptions of'smartness' and related ethical concerns in the home. *arXiv preprint arXiv:2005.00284*, 2020.

[33] Nataliya Shevchuk, Harri Oinas-Kukkonen, and Vladlena Benson. Risk and social influence in sustainable smart home technologies: A persuasive systems design model. In *Cyber Influence and Cognitive Threats*, pages 185–216. Elsevier, 2020.

[34] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, pages 65–80, 2017.

[35] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User perceptions of smart home iot privacy. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW):200, 2018.