Improving Adoption of Home IoT Beyond Single-Family Homes: Delineating Required Characteristics

Tushar M. Jois
City College of New York
tjois@ccny.cuny.edu

Susan Landau
Tufts University
susan.landau@tufts.edu

***Abstract*—Mass adoption of home IoT devices has been slower than expected, and numerous user studies have looked at issues consumers have regarding the use of these devices. But despite multiple studies on user concerns around the world regarding characteristics sought in home IoT devices, two important aspects have largely been missing. The first is the wide variety of housing types. Almost all user studies studying desired characteristics of home IoT devices have focused on the single-family stand-alone home environment. Wide adoption of home IoT devices, however, will mean use in a variety of living situations: rental apartments, condominiums, retirement communities, dormitories, and others. This introduces new complexities, including the second largely ignored issue. In these other types of housing situations, multiple other players are involved in the deployment of home IoT devices, including builders, landlords, housing managers, government regulators, and more. Getting home IoT devices right includes factoring in the characteristics that these other players desire and expect. This will be particularly critical in standardization efforts for home IoT.**

Previous work has shown that home IoT devices must satisfy obvious requirements of security, privacy, and interoperability – and less obvious ones of reliability, safety, data portability, usability, and controllability. Our work extends this list in in two important ways. First, by broadening the literature review to other previously ignored but highly relevant fields, including human-building interaction, we collect all previously studied characteristics relevant to home IoT. Second, we provide precise definitions of each; as a result of the analysis involved, we introduce new characteristics not previously considered by the computer science community. Our research in delineating required characteristics of home IoT provides a crucial building block for standardizing home IoT devices.

I. Introduction

In 1939, the magazine *Popular Mechanics* featured an article on "The Electric Home of the Future." George Bucher, the President of Westinghouse Electric and Manufacturing Company, imagined that people might light their home in ways that we discuss now: "warm white, daylight white, gold, red, blue, pink, green," with choices dependent on the user's mood [1]. Though the article envisaged multiple control centers from which the homemaker could command appliances "in the kitchen and laundry" and remote controls from one room to another were also part of the picture, true *smart devices* were not part of the discussion [1]; the modern computer was just in its infancy. A vision for the end-to-end *smart home* would have to wait until the 1960s cartoon program, The Jetsons. Realizing that vision would take somewhat longer.

We should not be surprised by this turn of events. We live in a world in which people's lives often appear to be completely integrated with their digital devices. But in the 1980s, office systems and personal computers were greatly underutilized [2], so researchers studied what factors cause users to adopt new technology. Fred Davis developed a behavioral model of user acceptance he called the "Technology Acceptance Model" (TAM) showing that "perceived ease of use" and "perceived usefulness" strongly fed into people's attitude towards using new technology [3]. The TAM model is empirically successful at predicting about 40% of a system's adoption.

In 2003, Legris et al. observed that factors regarding user adoption depend on the type of technology [4]. This makes sense: a remotely controllable home thermostat will have different requirements for ease of use and security than an IT system managing the spinning of nuclear centrifuges. Users take those various factors into account even when they do not explicitly say so. Early research in home IoT technologies often focused on solutions for the disabled and elderly, who could particularly benefit from home IoT technology, since this would enable them to age "in place." Studying a variety of efforts for this demographic, Chan et al. observed: "Further research is needed into legal and ethical problems, user and provider acceptance, and *user and provider requirements and satisfaction*" (italics added) [5].

The potential of home IoT technologies – increased convenience, security, energy efficiency, and ability to enable elderly and disabled individuals to safely reside in place – has long been discussed by engineers, futurists, businesspeople and others, yet the home IoT has been relatively slow to catch on. Early adopters have favored some types of home IoT tools (doorbell cameras, thermostats), but mass market adoption has not followed [6], [7]. In studies, residents have expressed concerns about security, privacy, reliability, and technological

Workshop on Security and Privacy in Standardized IoT (SDIoTSec) 2026
23 February 2026, San Diego, CA, USA
ISBN 978-1-970672-01-5
https://dx.doi.org/10.14722/sdiotsec.2026.23021
www.ndss-symposium.org

complexity [8], [7], [9], [10]. Smart devices often have more capabilities than their non-smart "equivalent," and living with home IoT devices brings new decisions and choices. Even home IoT device set up can be challenging.

Most of the complexity, however, arises from additional *characteristics* residents expect home IoT devices to support. Residents and regulators anticipate that introduction of a smart device will not create a safety hazard, that is, a smart version of a smoke or CO_2 detector should satisfy *safety* by being at least as safe as its non-smart counterpart. Introduction of a home IoT device should not decrease security; that is, device should have the characteristic of *device security*: being secure against attacks and exploits. In addition, residents seek *data portability* so that they easily transfer the settings of the smart device to a new residence. Device "smartness" introduces a layer of abstraction to a device, making *controllability* – enabling a resident to control who can set preferences on a home IoT device and data and what level of preferences the user can set – a desired characteristic. Resolving complexities will enable home IoT devices to function in satisfying ways for residents.

Residents will need to be satisfied for home IoT devices to be widely adopted, but so will others involved in home residential units. To date, most computer science research on home IoT devices and residents has concentrated on single-family standalone residences and their users. In future, of course, home IoT devices will also be used in other types of housing including rental units and group situations. These devices will also have to satisfy building owners, managers, and possibly even those living in neighboring residences. They will also need to satisfy regulatory requirements—is the device safe? secure? reliable? Such considerations are critical to the success of emerging standards for home IoT such as Matter [11]. Interests that may be aligned regarding a smart doorbell in a private home may be much less well aligned when there is a landlord and residents with different judgments regarding the appropriateness of photographing visitors.

Another distinction for home IoT devices when used in other than single-family home situations is that leasers' residences can be configured quite differently from those of home owners. A 2014 U.K. study on heating controls and domestic energy, for example, noted that renters are notably less likely to have a full set of heating controls than home owners [12]. In the U.S., renters are less likely to have energy-efficient appliances in their homes [13]. Mixed economic incentives lie behind these choices. So they will be for home IoT choices.

For rental apartments, condominiums, dormitories, retirement, communities, and other group arrangements, privacy within the residence versus safety or security of the shared building or controllability of home IoT devices when the owner of the device is likely to be different than for single-family homes. Where building managers and landlords might see an opportunity to keep their rented residences well run and safe, renters may fear loss of autonomy and privacy. Where providers of home IoT devices and smart speakers might see an opportunity to provide convenience, safety, or security, residents may fear surveillance in their home.

The field of human-building interaction (HBI) [14] has studied the interactions between stakeholders: occupants (residents, visitors), developers, and authorities, such as state and local regulators. These parties each have differing concerns about residences and weigh the characteristics that we will describe differently. The computer science focus on the users of home IoT devices and the characteristics they value has appeared to ignore the direction of HBI work. Yet, understanding the requirements stemming from owners/managers, developers, and authorities is crucial to standardization of home IoT devices in multi-family dwelling units.

There is an additional complexity. Even in a single-family standalone home, resident preferences for home IoT systems are not necessarily aligned. Thus, there may be conflicts about such basic issues as trade-offs between safety and security. The first step to resolving such conflicts is having a clear delineation of the preferred characteristics of home IoT devices by *all* involved parties. That is the intent of the current work.

Contributions. In this paper, we discuss the different characteristics participants in the home IoT space – residents, building, managers, landlords, device, developers, infrastructure providers, and government regulators – seek in home IoT devices. We make the following contributions:

- We perform a literature examination taking into account the work in other fields on the current state of home IoT, studying use cases, deployment scenarios, and the needs of end-users and other participants, revealing significant gaps in understanding. We consider various barriers to the widespread adoption of home IoT related to these gaps.
- Using this examination, we find that earlier definitions of desired characteristics for home IoT devices have been less than comprehensive and, at times, imprecise. We provide more precise definitions for desired home IoT characteristics than earlier work, also including several characteristics not previously considered in home IoT.
- We analyze the characteristics, describing potential interactions between them and implications for standardizing and deploying home IoT.

This work is exploratory. One of the difficulties that home IoT devices have in adoption is conflicts between desired characteristics, a problem faced in other computer science environments [15], [16]. Determining principles governing the resolution of such conflicts is essential for developing standards for home IoT devices; a necessary first step to doing so is having a full and clear description of required characteristics. That is the motivation behind this research, which we believe forms an essential foundation towards developing robust standards for home IoT devices.

II. The Current State of Home IoT

We now examine the literature to come to an understanding about the current state of home IoT, the devices that populate them, and the people who live in them. We take a broad view of home IoT, studying publication venues not typically studied by computer security/computer science researchers.

Such interdisciplinary breadth is necessary for understanding the type of characteristics sought in home IoT in multiple scenarios and therefore for standardization efforts.[1]

A. Defining the Smart Home

As Sovacool et al. point out, there are multiple definitions of what constitutes a smart home [18], from the 1992 definition by Lutolf of a residence with different surfaces sharing a calm communication system [19] to one by Marikyan et al. in 2019 of a residence capable of providing tailored services to each resident [20]. We choose to use Aldrich's middle-ground definition: "a residence equipped with computing and information technology, which anticipates and responds to the needs of the occupants, working to promote their comfort, convenience, security, and entertainment through the management of technology within the home and connections to the world beyond" [21]. This definition is "smarter" than a computer Internet hub, but is still simple enough to accommodate a home with only a few smart devices. Although these devices might not interact on a digital level, they could nonetheless interact on a physical one (as we will see in Section III-B). Thus, Aldrich's model presents the appropriate level of complexity of smart home for our concerns.

B. Uses of IoT Devices in the Smart Home

As Celik et al. note, IoT consists of "commodity devices that integrate physical processes with digital connectivity" [22]. The home IoT devices that comprise a smart home span a wide gamut of potential uses within this definition. Rather than listing all of these, which would be infeasible, we categorize devices into four broad *use cases*.

Resident safety. These are the set of devices that apply digital connectivity to *improve the physical safety of residents*. An example is the smart doorbell, which integrates a camera into a traditional doorbell, connecting it to the Internet. When a visitor rings the doorbell, the resident can verify the identity of a visitor through the video feed, perhaps speaking through the smart doorbell to ask the visitor's purpose. Many smart doorbells start recording if there is motion, alerting the resident to potential intruders. In these ways, a smart doorbell provides additional resident safety over traditional doorbells due to its always-on Internet connectivity. The smart doorbell can be deployed both in single-family settings (e.g., Ring [23]) and multi-unit buildings (e.g., ButterflyMX [24]).

This use case also includes devices that operate within the home such as a smart smoke detector. As with a smart doorbell, the always-on connection allows for better safety, since alerts can be sent remotely (even if no one is around to hear the alarm) while any maintenance issues (e.g., low battery) can be handled proactively. Moreover, such a device can be combined with other home IoT devices for even greater safety, e.g., a smart smoke alarm triggering a shutdown of the home's HVAC system via a smart thermostat (which we discuss below) to prevent smoke from spreading. This idea – interoperating devices for increased functionality – is core to the promise and potential of home IoT [22].

Building security. These are the set of devices that apply digital connectivity to *improve the physical security of the building containing the devices*. An example is the smart lock, which can have a keyhole like a traditional (non-smart) lock, but typically also presents an alternative interface such as a keypad or biometric scanner that can be remotely configured. The smart lock provides additional security as it enables *revocation of access without replacing the lock*. In a typical lock, access is granted by sharing a physical key; on the other hand, with a smart lock, the device owner can provide a code to a visitor. This provides a useful security benefit over the non-smart lock to handle the cases of temporary visitors (such as a repairperson), tenants (such as in an apartment), and guests (such as in a hotel or short-term rental) – with a smart lock, they cannot re-use their credentials after their visit.

Devices that provide building security can also provide resident safety. A smart doorbell (discussed above) also provides building security by acting as a deterrent against vandals and trespassers. Another device, a smart water leak detector, can also help stop water damage to the building early (building security) as well as help detect flooding before it impacts the residents (resident safety). The class of resident safety devices is broader than building security devices, however (e.g., a smart carbon monoxide detector is more about resident safety than building security). Notably, the two are also treated by regulators differently; safety inspections are a standard aspect of licensing a residence for occupancy, but security is not.

Resident convenience. These are the set of devices that apply digital connectivity to *improve the convenience of the residents when controlling physical aspects of their home*. These straightforward devices are the most commonly discussed when considering home IoT. An example is the smart thermostat, which enables setting temperature and configuring schedules for HVAC operation, much like a non-smart thermostat. Internet connectivity allows a resident to control the thermostat from anywhere. Smart thermostats offer room-level temperature monitoring (e.g., to handle the temperature differences between the upstairs and downstairs) and automatic adjustment of temperature (e.g., due to demand response events from the energy grid) [25], as well as coordination with other devices (e.g., in the smart smoke detector example above). For landlords, a smart thermostat can ensure that certain HVAC policy is met without manual inspection (e.g., ensuring the heating is on at a minimum temperature to prevent pipes freezing) [26]; this overlaps a bit with building security.

Many home IoT devices provide additional convenience over non-IoT counterparts; deployment of such devices is widespread [27]. Smart appliances, for instance, promise more fine-grained control over cooking and food handling, such as a smart refrigerator that recommends when food inside is close to expiry. Smart vacuums automatically can roam the home, building an understanding of the layout of the house and its

[1] For a review of the technical computer science literature in home IoT security, see Alrawi et al. [17].

occupancy schedule to optimize its cleaning routine without resident intervention. Smart speakers allow for easier control over other smart home functions.

Resident entertainment. This is the set of devices that applies digital connectivity to *make the resident's living experience more enjoyable* – a major motivation behind home IoT adoption [28]. Such a device is a smart light, which allows remote control of an LED-based bulb. Smart lights have notable features that support other use cases, such as remote on (e.g., to imitate presence for building security) and off (e.g., for energy savings and convenience). The entertainment (or fun) aspect comes from the smart light's ability to change colors remotely and be programmed in patterns. For instance, a resident may want a strobe effect for a party or a soft pulsing orange glow for a romantic dinner at home. The smart bulb's connectivity allows this kind of control and therefore enjoyment. Multiple-purpose home IoT devices can also provide entertainment, e.g., a smart speaker that reads audiobooks out loud.

C. Home IoT Deployment Scenarios

Home IoT systems have typically been designed for a standalone single-family environment where the device owner is a resident. Early home IoT systems had a fixed mapping between a home IoT device to a smartphone and therefore had minimal support for adding users who were not the owner [29]. A push towards cloud-backed home IoT platforms has led to multi-user authentication schemes [30]. While these create a distinction between the owner and a resident, they assume that the two are at least a part of the same family unit.

There are, however, many scenarios where the owner and resident are completely distinct. Consider rental situations, such as when landlords deploy home IoT technologies (e.g., thermostats, sensors) in spaces occupied by tenants, including short-term ones such as Airbnb guests. The smart device owner is no longer the resident. Sovacool et al. studied home IoT through focus groups and surveys of U.K. adults, breaking down housing status between full homeowners, homeowners with mortgages, public housing tenants, and private housing tenants [31]. Their study found that tenants were more likely to view home IoT as the domain of the more affluent [31].

There are other cases where this owner-resident relationship is more nebulous, such as assisted living facilities or dormitories. But while there is initial research in landlord-tenant scenarios, there is a paucity of research in alternative settings for home IoT. Indeed, as Koupaei and Cetin note, home IoT is currently not suitable for "secondary users" (i.e., residents who are not owners) and usability for these secondary users is limited [26]. For example, in their study, Koupaei and Cetin found that owners were disappointed that they could not provide their guests with access to their smart thermostat during their stay [26]. Other studies with secondary user groups highlight this unsuitability, such as those with visitors to a smart home [32], [33], nannies [34], [35], and short-term rental guests [36], [37]. Also, there is limited work on the issues surrounding those who enter the house to perform maintenance on home IoT devices, although recent work has looked at its privacy implications [38], [39].

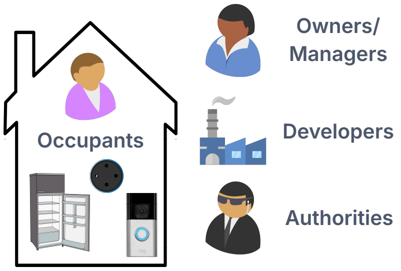

Fig. 1. The stakeholders in home IoT, as inspired by work in human-building interaction [14]. Note that unlike prior work, we explicitly separate owners/managers of buildings from the residents, as owners/managers have different incentives (and therefore install different devices) from residents.

The questions we are exploring fit within the studies of human-building interaction (HBI), an interdisciplinary field that studies how building affect people and how people "design, interact with, adapt to, and affect the built environment and its systems" [14]. Taking the point of view of HBI as an academic field, Bercerik-Gerber et al. classifies the stakeholders as occupants, researchers, developers, and authorities [14]. We build on their general classification, but, taking in account the discussion above, we add (building) owners/managers to the list and remove researchers. We visually represent these stakeholders in Figure 1.

D. How Users Perceive Home IoT

We now discuss literature that investigates user perceptions towards home IoT deployments.

The perception of reliability in home IoT has consistently been the most important for users. In 2013, Balta-Ozkan et al. interviewed adults in the U.K. about home IoT, concluding that there was a belief that home IoT technology was not sufficiently reliable for adoption [8]. This belief is widespread across the world as well as persistent over time. For instance, a later study of Korean users who specifically resisted home IoT deployments found that reliability and trustworthiness were key factors that explained their resistance [7]. A broader study of adults in E.U. countries and Russia found that users are wary of the wide variety of device manufacturers and their different communication platforms believing that the devices lack the reliability necessary for a large-scale deployment [40].

In addition, the literature shows that users also emphasize the privacy implications of home IoT. Schomakers, Biermann, and Ziefle studied how home automations impact perceptions of privacy through interviews with German adults. They found that the higher degree of automation in a smart home, the more concerns users had with privacy and trustworthiness [9]. A follow up study by Schomakers, Lidynia, and Ziefle surveyed users about several technologies in the IoT space (including home IoT) and found that users were willing to set aside privacy concerns and accept IoT devices only when they feel the perceived benefits outweighed the perceived sensitivity of the information disclosed by these devices [41]. This result is in line with the study of Korean users noted above. In that study, privacy was especially relevant to those users who *reject* home IoT outright (instead of postponing adoption until technology improves) [7]. For these users, the perceived benefits *could not* mitigate the perceived privacy risk, and they refused to adopt home IoT as a result.

Reliability and privacy, while important, are not the only qualities the academic community studies. Another survey of adults in Germany by Schomakers et al. showed that users found reliability and privacy important, but also sought greater control over their data and systems than currently available [42]. A recent innovative study of 7.5 years of Australian tweets on home IoT showed that users repeatedly raised issues regarding control of home IoT and the potential for misuse by malicious actors [43].

E. Barriers to Widespread Home IoT Adoption

Despite established use cases, home IoT has not seen significant adoption. As such, significant work has been done to assess barriers to adoption by understanding the impact of the user perceptions discussed above. Shin et al. interviewed Korean users and determined that compatibility between devices and privacy are necessary aspects of the TAM for home IoT [44]. Nikou supplements the TAM with the related "innovation diffusion theory" to identify the interrelated properties of compatibility, trialability, and observability as necessary for adoption [45]. Cognitive dissonance has also been used to failure to adopt home IoT; a user study found that when home IoT expectations are not met, this creates dissonance users resolve by discontinuing use of home IoT [46].

In addition to the use of existing models, work in the literature have constructed new frameworks to understand adoption specific to home IoT. Hong et al. developed a model with four types of "perceived risk" (performance, financial, privacy, psychological), finding that only financial risk had an impact in increasing resistance to home IoT [7]. FakhrHosseini et al. interviewed 21 experts in home IoT to construct a set of standards and a unifying framework to drive home IoT adoption, finding that safety was considered paramount in all existing approaches to standardization and regulation [47].

A major meta-analysis by Markiyan et al. shows that the barriers to home IoT adoption are due to key gaps in understanding in terms of user-centric research, technical-centric research, home IoT adoption, and regulations [20]. Their work mentioned that while factors such as usability and reliability are well-studied, home IoT systems are complex, which has hindered IoT adoption [20]. Markiyan et al. noted that security and privacy risks, as well as a lack of interoperable systems, are major inhibitors to acceptance and adoption [20].

III. The Characteristics of Home IoT

Here we discuss the *characteristics* of home IoT devices and deployments. Each is essentially a requirement that home IoT stemming from expectations of users, developers, and regulators. These characteristics arise from home IoT literature. To focus on the characteristics that arise from more complex home IoT deployments – and not simply be an encyclopedia on the various possible applications of home IoT devices – we do not include a full history of the study of each of the characteristics. Instead, we introduce them, citing notable research that first isolated them.

A. Developing the Characteristics

When considering the sensitive applications of home IoT (i.e., to residents and buildings), as well as the sensitive data home IoT devices collect (i.e., from residents and buildings), *security* and *privacy* emerge as necessary and obvious characteristics [9], [7], [41]. In the home IoT context, security has typically meant device security in the sense of secure against cyberattack [17]. But home IoT devices are part of a "cyber-physical system" that control physical devices. In discussing security, it is important to distinguish between *device security* (the home IoT device is operating securely) and *building security* (the home is secure as a result of the device, e.g., via smart locks [48]); both are desirable but are different concerns.

We consider *resident safety* as a separate characteristic; this covers the class of devices for which the resident is safe due to the device's operation (e.g., via smart doorbells [23], [24]). As mentioned previously, the experts consulted by FakhrHosseini et al. all agreed that resident safety was paramount [47].

When considering user perception, the literature shows the *reliability* repeatedly raised by users as the most important characteristic: users are concerned if current systems are reliable enough for adoption [8], [7], [40]. Studies on user perceptions also introduce related notions of *usability* (perceived ease of use) [29], [30] and *value* (perceived usefulness) [45].

Data portability also matters. A quintessential example is smartphones. When someone buys a new phone, they want their contacts, preferences, and other data to "port" over to the new device. A less quintessential example, but similarly important to a home resident, is porting information for such devices as smart thermostats to a new device. What people typically seek to port over is "functionality" rather than content: smart thermostat heating and cooling schedule, not the history of use. While people typically change their home less frequently than they change their smartphone, people, especially renters, do move, making data portability relevant.

When considering the barriers to adoption, we find that two more technically oriented characteristics arise: *controllability* of the home IoT devices, as well as the *interoperability* between them. While these concerns are not necessarily top-of-mind for users, they are relevant for the wide-spread deployment of home IoT [22] and in the development of home IoT standards such as Matter [11].

B. Defining the Characteristics

Below, we enumerate these characteristics and provide definitions of each with associated context.

Reliability. We define this characteristic as *the dependability of the home IoT system.* Moore et al. state that this characteristic encompasses device, network, and system reliability [49]. As noted in several of the user studies described in Section

2, reliability is by far the most important acceptance criterion for home IoT in the minds of users [8], [7], [40]. Users expect home IoT devices to function when necessary; for some types of devices, such as smart sensors, this must be all the time. To ensure reliability, home IoT devices are thus required to be *resilient*, e.g., incorporate guardrails against the failure to function. For instance, a smart smoke detector might inform a resident that it has low battery (i.e., will fail within a short period) by sending a notification to their smartphone, as well as by periodically emitting an annoying beeping sound.

Reliability is also related to the choice of components that comprise a home IoT device. The scope includes the quality of physical components (from the types of plastic casings that house the device to the semiconductor manufacturing process used for the device's system-on-chip) but also the technical architecture of the home IoT device. For example, many home IoT devices are backed by the cloud, which handles data storage and processing. A good example of such a device is a smart security camera which streams video to the cloud, reducing the computing power required on-device. But these devices fail when the network or cloud is unavailable, tying their reliability to an external component rather than internal ones. Indeed, for this reason, the emerging Matter home IoT connectivity standard eschews relying on the cloud [11].

Device security. We define this characteristic as *the cybersecurity of home IoT devices, that is, devices are secured against cyberexploits, cyberattacks, and the interactions of cyber-physical aspects of other home IoT devices*. Device security failures can lead to information disclosure and possible hijacking of the home IoT system by attackers [50], [51], [52], [53] and therefore requires defenses [54]. In this sense, home IoT devices are not unlike other IT systems. But in another, they have at least three major differences. Home IoT devices are low powered and with little storage, thus obviating security protections that larger systems can afford; there will be trillions of them; and they will be used largely by technically unskilled people with little tech support. The potential risk for large-scale exploitation is high. As the Mirai botnet showed, this can have serious consequences [52].

Resident safety. We define this characteristic as *the freedom from physical harm due to the function of a home IoT device*. For example, a smart smoke detector provides safety for the residents of a home by continuously monitoring the air for signs of fire. Not all home IoT devices are as safety critical as a smoke detector. But as cyber-physical systems, many have the potential to impact resident safety. A smart refrigerator, for instance, can help improve resident safety by informing residents if any food inside it is past its expiration date.

Building security. We define this characteristic as *the freedom from physical damage to a facility due to the function of a home IoT device*. For example, a smart water leak detector helps detect potential flooding early, before any major damage is done to building walls or floors. We note that this definition also can provide the security of *residents*. A smart door lock helps protect the building against trespassers and provides residents protections against thieves. This in turn can bolster resident *safety* as well, but this characteristic is separate and arises *because of* building security.

Guardrails are especially relevant in cases where failure of a home IoT device may create *additional* risks over failure of a non-IoT device of the same type. Consider, for instance, a smart stove permitting remote oven pre-heating (unlike a traditional kitchen stove with physical controls). Such a device must have an automatic shut-off timer along with remote pre-heating. Otherwise, the oven may stay on for days, if, for example, a resident remotely turns the oven on to have it ready when they return home——but then goes straight out to dinner from work, forgetting they turned on the oven and thus creating a safety hazard. In this way, the smart device introduces a new type of risk: an indefinitely pre-heating oven.

Privacy. We define this characteristic as *the conformance of a given information exchange to contextual information norms*, in line with Nissenbaum's definition [55]. Understanding the norms is key to understanding if a system meets this quality. For example, a landlord learning through home IoT of residents' water usage could be considered within norms, but the landlord's sharing that information with a prospective landlord of the tenant(s) would not be.

Interoperability. We define this characteristic as *the ability of home IoT devices to seamlessly exchange information and operate on this information with each other or through an intermediary*. Various home IoT vendors have created cloud-backed platforms that allow for coordination between home IoT devices. Examples include If This Then That (IFTTT), Samsung SmartThings, Amazon Alexa/Echo, Apple HomePod, and Google Home [56]. These platforms enable home automation, in which devices communicate with each other to provide a greater function. For example, a popular IFTTT home automation triggers smart lights to turn blink if the smart doorbell is rung.

To improve interoperability, several home IoT technology vendors have convened a standards-making body, the Connectivity Standards Alliance, consisting of component manufacturers (e.g., Nordic Semiconductor), device manufacturers (e.g., Siemens), Internet service providers (e.g., Comcast), platform developers (e.g., Google), retailers (e.g., IKEA), among others [57]. The resulting Matter protocol provides a set of interfaces designed to be interoperable across device types and manufacturers, and has been shown to have strong interoperability properties [58].

The above discussion focuses on the *digital* interoperability of home IoT devices and is concerned with the communication between devices. But, as home IoT devices are cyber-physical systems, we must also consider *physical* interactions as well. Celik et al. provide an illustrative example. Consider how use of the "simulate-occupancy" app, used by a resident to simulate home occupancy while away, might turn on lights in the front hallway; then a "welcome-home" app might activate the "at-home" mode for the system. The latter could then activate the "home" app, which turns on the HVAC to "at-home" settings and unlocks the patio door. In this instance, interaction in the *digital* domain can lead to an unintended interaction in the *physical* domain [22].

Usability. We define this characteristic as *the ability of home administrator(s)* and *home user(s) to easily manage the controls of home IoT systems*. This distinction is important, as the two types of users differ in their concerns in a smart home setting [59]. Usability is a characteristic that needs to apply during all phases of the home IoT device lifecycle—commissioning, changes in ownership, use, or location, decommissioning—and not just when it is used for its primary function in addition, a home IoT device should have a useable commissioning process when installed and a useable decommissioning process when removed.

Digital devices should be designed to be both digitally and physically usable. Consider a smart lock purchased for a house's front door. As with the installation of any new lock, the front door may need to be re-bored to fit the new lockset, and so the smart lock should be reasonably standard in shape and size to enhance usability. In addition to the *physical* installation process, the device must also go through the *digital* installation process of connecting the smart lock to the network and registering for an account, which also must usable.

Data portability. We define this characteristic as *the ability to obtain settings and history of use data and transfer it to a comparable platform*. Note that this characteristic is not currently active industry practice even when required by law. Although GDPR Article 20 provides for swapping devices between platforms, a recent study by Turner and Tanczer indicates this is not currently occurring in practice [60].

A change in platform may also occur when the residents of a smart home change. From a device perspective, we consider two sub-classes: data portability for devices *fixed* in a smart home, and data portability for devices *moveable* between smart homes. Fixed devices are owned by the owner of a given smart home remain in the space, regardless that residents change over time. Users access and transfer preferences to fixed devices when they take up residence in the space. An example of a fixed device is a smart thermostat in an apartment; these are typically bolted into the wall and configured for temperature and schedule when a new tenant moves in.

In contrast, movable devices are brought into the space when a user takes up residence and leave when the residents moves out. An example here would be a smart speaker, which is small enough to move with the user as they change apartments. When these new devices enter a smart space, though, they should be able to interact with any existing (fixed) devices — a property that overlaps with interoperability, discussed above.

Controllability. We define this characteristic as *the ability of a resident to control who has access to device preferences and data, and what level of access they have to the functionality of the device*. A useful example is to consider controllability for a smart thermostat. For deciding who has access, parents and the household's older children may want access to control the thermostat. But, for deciding the level of access, perhaps the parents want to have temperature control over the whole house, allowing older children control only in their bedrooms. Complexity is added if the smart home is a rental unit; the landlord may require a higher level of access to configure maximum and minimum temperatures that can be set [26]. Visitors, such as babysitters or maintenance staff, raise new issues, especially in relation to the access they need to do their jobs [34], [35], [39].

As a characteristic, controllability does not make any statement on who *should* have what access level, but rather if the home IoT device makes such fine-grained control *available*. Resolving these issues is itself a complex issue (i.e., between competing stakeholders and their needs) and requires understanding possible interactions between controllability and the other characteristics such as privacy (e.g., a landlord viewing the preferences of tenants).

IV. Discussion

We now provide analysis and insights for future efforts.

Interactions between characteristics. We have attempted to present the characteristics in Section III in a general order based users' concerns in the literature. In many cases, however, these characteristics interact with one another and result in additional complexity. Consider, for instance, reliability and privacy. Having a smart fridge in an apartment log all activity helps a repairperson diagnose a problem and thus supports device reliability [54] – but who should be permitted to view a device's activity log [39]? There is a clear conflict here: prioritizing one of the characteristics (e.g., allowing the landlord to view the logs) potentially hinders the other (e.g., revealing information on the renter's day-to-day activities).

Conflicts between required characteristics are not unique to the home IoT setting. In the early 2000s, Clark et al. wrote about the "tussle in cyberspace" [15] that was emerging over the deployment of Internet infrastructure. The conflicts between pairs of characteristics arose due to different stakeholders in the early Internet having competing interests behind desired choices, e.g., the desires of Internet service providers to lock in customers, and the desires of customers to switch Internet service providers [15].

We perceive similar conflicts in the home IoT space. Continuing with our example above, the question of access to home IoT logs is a conflict between the characteristics of reliability and privacy. Indeed, these two characteristics are fundamentally in conflict, and the conflict cannot be simply resolved by a straightforward reconfiguration of the smart home. A choice must be made, and the question of who makes it – residents? owners? manufacturers? standards bodies? – is open. Clark et al. propose design principles for resolving these conflicts, but solutions for Internet infrastructure are almost certainly different than those for home IoT. Thus, future work must systematically evaluate home IoT as a "tussle space" (in the manner of Clark et al. [15]) and attempt to derive coherent principles towards resolving them.

Of course, not all interactions between characteristics necessarily result in conflict. For example, consider an automation that unlocks the back door to the terrace once the front door is unlocked. In a upper-floor apartment, this may not be a safety issue, but on a ground-floor apartment, it would be. Based on the characteristic of data portability, when a resident moves from an old domicile to a new one, they can move their settings with them. If the automation is ported to a ground-floor residence, automation poses concern. But rather than a confict between data portability and resident safety, this is instead an *edge condition* that involves two characteristics. This is less about a conflict needing resolution, and more of a technical concern about interpreting home IoT preferences in different contexts that can be resolved by purely technical means [22]. Similarly, the greater interoperability recommended by standards like Matter can lead to unintended device security vulnerabilities in implementations [61], [62]; this is not so much a conflict as it is the well-known difficulty of translating a standard into a software implementation.

There are also cases where two characteristics align well with each other. A good example is resident safety and interoperability; better interoperability between monitoring devices (e.g., for fire, water leaks, etc.) will lead to a better understanding of the conditions in a home and thereby enhance resident safety in emergencies.

Value and the characteristics. In addition to the characteristics we describe in Section III, there is one pseudo-characteristic we wish to discuss: *value*, or the perceived usefulness of the device based on its price. We do not consider it to be a full characteristic because value is, so to speak, in the eye of the beholder, i.e., the person who purchases it. Unlike other characteristics, value is determined solely by someone with an interest in the device's functionality. A resident or owner will purchase a device if they believe the functionality the device provides is worth the cost.

Device manufacturers take value into account as they decide on features to include in a home IoT device. Because lower-priced items sell better, device manufacturers minimize the quality of some characteristics (or skip having them) and/or recoup product costs by selling customer data. Value interacts with *all other characteristics* in the aggregate, rather than having a specific conflict with *an individual characteristic*. As such, it must be considered separately.

V. Impact on Standardization

Standardization efforts in home IoT such as Matter focus on providing interoperability while also incorporating device security their core specifications [11]. Academic research has also investigated how to add privacy compliance to Matter [63]. But the other characteristics we identify are just as crucial for Matter's deployment and adoption but have not fully considered to date. For instance, resident safety is clearly paramount, but required functionality or guardrails for safety-critical home IoT devices have not been definitively standardized. As another example, home IoT standards often conflate data portability with interoperability [60], but it is a distinct characteristic – changing platforms, rather than connecting them – and requires specific technical solutions. More work is therefore required to better incorporate the characteristics into emerging home IoT standards.

Handling the conflicts between characteristics across home IoT is also a key concern for standardization. A simple solution would be to always prioritize device security, even if it comes at the expense of other characteristics. This stance is the one typically taken by work in the academic security literature, as well as by industry bodies for other technologies [64]. But, it is not clear that this decision would make sense in home IoT. For instance, would it be appropriate to prioritize device security, even at the expense of interoperability, in home IoT? The answer is not as clear, since interoperability is often the *reason* to purchase a device, i.e., for home automations that provide resident convenience or entertainment. Thus, creating thoughtful principles for prioritizing the characteristics specific to home IoT is critical to ongoing deployment and standardization efforts; we see our work setting up the characteristics as a first step towards this.

VI. Conclusion

It is natural that computer science research on the adoption of home IoT devices initially focused on the characteristics that residents sought. After all, if residents do not want a device, they will not use it, will not buy it, and might not even rent or purchase a location that has such devices in it. So it makes sense that researchers would focus on residents' preferences regarding required characteristics for home IoT devices. But as we noted earlier, single-family standalone homes are not the sole types of residences in which people live; indeed, in many parts of the world, apartment buildings are the norm. Once one starts to look at residences aside from single-family standalone homes, other stakeholders come into the picture. The other stakeholders—builders, landlords, managers, regulators—have different sets of criteria than owner/residents do. These characteristics come into conflict, and standardization will need to handle that conflict.

In future work, we look at the conflicts between these characteristics. To understand and resolve these conflicts, we must first have a clear listing and understanding of the desired characteristics for home IoT devices. Our work, by looking not just at residents, but considering also the needs of owners different from the residents, and regulators, who are responsible for ensuring safety and security of people's residences, expands and clarifies the list of characteristics and their definitions. Thus, this work represents an important step towards standardization of home IoT devices.

Acknowledgments

The authors are grateful to participants of TPRC53 and to David Kotz, who provided useful comments on preliminary versions of this work. This work is supported by National Science Foundation awards 1955805 and 1955172. The views and conclusions contained herein are those of the authors and should not be interpreted as those of NSF. Any mention of specific companies or products does not imply endorsement by the authors, their employers, or NSF.

References

[1] G. Bucher, "The Electric Home of the Future," *Popular Mechanics*, vol. 72, no. 2, August 1939.

[2] D. M. S. Lee, "Usage Pattern and Sources of Assistance for Personal Computer Users," *MIS Quarterly*, pp. 313–25, 1986.

[3] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, "Technology acceptance model," *J Manag Sci*, vol. 35, no. 8, pp. 982–1003, 1989.

[4] P. Legris, J. Ingham, and P. Collerette, "Why Do People Use Information Technology? A Critical Review of the Technology Acceptance Model," *Information & Management*, vol. 40, no. 3, pp. 191–204, 2003.

[5] M. Chan, D. Estève, C. Escriba, and E. Campo, "A Review of Smart Homes—Present State and Future Challenges," *Computer Methods and Programs in Biomedicine*, vol. 91, no. 1, pp. 55–81, 2008.

[6] S. J. Darby, "Smart Technology in the Home: Time for More Clarity," *Building Research & Information*, vol. 46, no. 1, pp. 140–47, 2018.

[7] A. Hong, C. Nam, and S. Kim, "What Will Be the Possible Barriers to Consumers' Adoption of Smart Home Services?" *Telecommunications Policy*, vol. 44, no. 2, p. 101867, 2020.

[8] N. Balta-Ozkan, R. Davidson, M. Bicket, and L. Whitmarsh, "Social Barriers to the Adoption of Smart Homes," *Energy Policy*, vol. 63, pp. 363–74, 2013.

[9] E.-M. Schomakers, H. Biermann, and M. Ziefle, "Understanding Privacy and Trust in Smart Home Environments," in *International Conference on Human-Computer Interaction*. Cham: Springer, 2020, pp. 513–32.

[10] W. Li, T. Yigitcanlar, I. Erol, and A. Liu, "Motivations, Barriers and Risks of Smart Home Adoption: From Systematic Literature Review to Conceptual Framework," *Energy Research & Social Science*, vol. 80, p. 102211, 2021.

[11] Connectivity Standards Alliance, "Matter FAQ," https://csa-iot.org/all-solutions/matter/matter-faq/, 2025.

[12] A. Munton, A. Wright, P. Mallaburn, and P. Boait, "How Heating Controls Affect Domestic Energy Demand: A Rapid Evidence Assessment," DECC, London, Report to the Department of Energy and Climate Change, 2014.

[13] X. Xu and C. Chien-fei, "Energy Efficiency and Energy Justice for U.S. Low-Income Households: An Analysis of Multi-Faceted Challenges and Potential," *Energy Policy*, vol. 128, 2019.

[14] B. Bercik-Gerber *et al.*, "Ten Questions Concerning Human-Building Interaction Research for Improving the Quality of Life," *Building and Environment*, vol. 226, p. 109681, 2022.

[15] D. D. Clark, J. Wroclawski, K. R. Sollins, and R. Braden, "Tussle in Cyberspace: Defining Tomorrow's Internet," in *Proceedings of the 2002 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, 2002, pp. 347–56.

[16] Trusted Computing Group, "Design, Implementation, and Usage Principles Version 2.0," Tech. Rep., 2005, december 2005.

[17] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, "SoK: Security Evaluation of Home-Based IoT Deployments," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 1362–1380.

[18] B. K. Sovacool and D. D. F. D. Rio, "Smart Home Technologies in Europe: A Critical Review of Concepts, Benefits, Risks and Policies," *Renewable and Sustainable Energy Reviews*, vol. 120, p. 109663, 2020.

[19] R. Lutolf, "Smart Home Concept and Integrations of Energy Meters into a Home Based System," in *Seventh International Conference on Metering Apparatus and Tariffs for Electricity Supply*. IET, 1992, pp. 277–78.

[20] D. Marikyan, S. Papagiannidis, and E. Alamanos, "A Systematic Review of the Smart Home Literature: A User Perspective," *Technological Forecasting and Social Change*, vol. 138, pp. 139–54, 2019.

[21] F. K. Aldrich, "Smart homes: past, present and future," in *Inside the smart home*. Springer, 2003, pp. 17–39.

[22] Z. B. Celik, G. Tan, and P. D. McDaniel, "IoTGuard: Dynamic Enforcement of Security and Safety Policy in Commodity IoT," in *NDSS*, 2019.

[23] Ring, "Neighbors by Ring: Neighborhood Security in Your Hands," https://ring.com/ca/en/neighbors, 2024, accessed: 2024.

[24] ButterflyMX, "Watch How ButterflyMX Works," https://butterflymx.com/how-it-works, 2025.

[25] H. Stopps and M. F. Touchie, "Residential Smart Thermostat Use: An Exploration of Thermostat Programming, Environmental Attitudes, and the Influence of Smart Controls on Energy Savings," *Energy and Buildings*, vol. 238, p. 110834, 2021.

[26] D. M. Koupaei and K. Cetin, "Smart Thermostats in Rental Housing Units: Perspectives from Landlords and Tenants," *Journal of Architectural Engineering*, vol. 27, no. 4, p. 04021042, 2021.

[27] D. Kumar, K. Shen, B. Case, D. Garg, G. Alperovich, D. Kuznetsov, R. Gupta, and Z. Durumeric, "All Things Considered: An Analysis of IoT Devices on Home Networks," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 1169–85.

[28] H. Sequeiros, T. Oliveira, and M. A. Thomas, "The impact of iot smart home services on psychological well-being," *Information Systems Frontiers*, vol. 24, no. 3, pp. 1009–1026, 2022.

[29] B. Ur, J. Jung, and S. Schechter, "The Current State of Access Control for Smart Devices in Homes," in *Workshop on Home Usable Privacy and Security (HUPS)*, 2013, pp. 209–18.

[30] W. He, M. Golla, R. Padhi, J. Ofek, M. Dürmuth, E. Fernandes, and B. Ur, "Rethinking Access Control and Authentication for the Home Internet of Things (IoT)," in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 255–72.

[31] B. K. Sovacool, M. Martiskainen, and D. D. F. D. Rio, "Knowledge, Energy Sustainability, and Vulnerability in the Demographics of Smart Home Technology Diffusion," *Energy Policy*, vol. 153, p. 112196, 2021.

[32] K. Marky, S. Prange, F. Krell, M. Mühlhäuser, and F. Alt, ""You Just Can't Know About Everything": Privacy Perceptions of Smart Home Visitors," in *Proceedings of the 19th International Conference on Mobile and Ubiquitous Multimedia*, 2020, pp. 83–95.

[33] K. Marky, N. Gerber, M. G. Pelzer, M. Khamis, and M. Mühlhäuser, ""You Offer Privacy Like You Offer Tea": Investigating Mechanisms for Improving Guest Privacy in IoT-Equipped Households," *Proceedings on Privacy Enhancing Technologies*, 2022.

[34] J. Bernd, R. Abu-Salma, and A. Frik, "Bystanders' Privacy: The Perspectives of Nannies on Smart Home Surveillance," in *10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20)*, 2020.

[35] R. Abu-Salma, J. Choy, A. Frik, and J. Bernd, ""They Didn't Buy Their Smart TV to Watch Me with the Kids": Comparing Nannies' and Parents' Privacy Threat Models for Smart Home Devices," *ACM Transactions on Computer-Human Interaction*, vol. 32, no. 2, pp. 1–53, 2025.

[36] S. Mare, F. Roesner, and T. Kohno, "Smart Devices in Airbnbs: Considering Privacy and Security for Both Guests and Hosts," *Proceedings on Privacy Enhancing Technologies*, 2020.

[37] Z. Wang, D. Y. Huang, and Y. Yao, "Exploring Tenants' Preferences of Privacy Negotiation in Airbnb," in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023, pp. 535–51.

[38] D. Anthony, C. A. Gunter, W. He, M. Khanafer, S. Landau, R. Mangar, and N. Reitinger, "The handytech's coming between 1 and 4: Privacy opportunities and challenges for the iot handyperson," in *Proceedings of the 22nd Workshop on Privacy in the Electronic Society*, 2023, pp. 129–134.

[39] W. He, N. Reitinger, D. Anthony, C. Bruno, S. Landau, C. A. Gunter, M. Khanafer, and R. Mangar, "Help Me Help You: Privacy Considerations for Third Party IoT Device Repair," in *Privacy Enhancing Technologies Symposium 2025*, 2025.

[40] E. Korneeva, N. Olinder, and W. Strielkowski, "Consumer Attitudes to the Smart Home Technologies and the Internet of Things (IoT)," *Energies*, vol. 14, no. 23, p. 7913, 2021.

[41] E.-M. Schomakers, C. Lidynia, and M. Ziefle, "The Role of Privacy in the Acceptance of Smart Technologies: Applying the Privacy Calculus to Technology Acceptance," *International Journal of Human–Computer Interaction*, vol. 38, no. 13, pp. 1276–89, 2022.

[42] E.-M. Schomakers, H. Biermann, and M. Ziefle, "Users' Preferences for Smart Home Automation–Investigating Aspects of Privacy and Trust," *Telematics and Informatics*, vol. 64, p. 101689, 2021.

[43] W. Li, T. Yigitcanlar, A. Nili, W. Browne, and F. Li, "Responsible Smart Home Technology Adoption: Exploring Public Perceptions and Key Adoption Factors," *Internet of Things*, p. 101622, 2025.

[44] J. Shin, Y. Park, and D. Lee, "Who Will Be Smart Home Users? An Analysis of Adoption and Diffusion of Smart Homes," *Technological Forecasting and Social Change*, vol. 134, pp. 246–53, 2018.

[45] S. Nikou, "Factors Driving the Adoption of Smart Home Technology: An Empirical Assessment," *Telematics and Informatics*, vol. 45, p. 101283, 2019.

[46] D. Marikyan, S. Papagiannidis, and E. Alamanos, "Cognitive Dissonance in Technology Adoption: A Study of Smart Home Users," *Information Systems Frontiers*, vol. 25, no. 3, pp. 1101–23, 2023.

[47] S. FakhrHosseini, C. Lee, S.-H. Lee, and J. Coughlin, “A Taxonomy of Home Automation: Expert Perspectives on the Future of Smarter Homes,” *Information Systems Frontiers*, pp. 1–18, 2024.

[48] S. Mamonov and R. Benbunan-Fich, “Unlocking the Smart Home: Exploring Key Factors Affecting the Smart Lock Adoption Intention,” *Information Technology & People*, vol. 34, no. 2, pp. 835–61, 2021.

[49] S. J. Moore, C. D. Nugent, S. Zhang, and I. Cleland, “IoT Reliability: A Review Leading to 5 Key Research Directions,” *CCF Transactions on Pervasive Computing and Interaction*, vol. 2, no. 3, pp. 147–63, 2020.

[50] E. Fernandes, J. Jung, and A. Prakash, “Security analysis of emerging smart home applications,” in *2016 IEEE symposium on security and privacy (SP)*. IEEE, 2016, pp. 636–654.

[51] K. Kafle, K. Moran, S. Manandhar, A. Nadkarni, and D. Poshyvanyk, “A study of data store-based home automation,” in *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy*, 2019, pp. 73–84.

[52] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric *et al.*, “Understanding the Mirai Botnet,” in *26th USENIX Security Symposium (USENIX Security 17)*, 2017, pp. 1093–1110.

[53] A. Rostami, M. Vigren, S. Raza, and B. Brown, “Being Hacked: Understanding Victims’ Experiences of IoT Hacking,” in *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, 2022, pp. 613–31.

[54] Q. Wang, W. U. Hassan, A. Bates, and C. Gunter, “Fear and Logging in the Internet of Things,” in *Network and Distributed Systems Symposium*, 2018.

[55] H. Nissenbaum, “Privacy as Contextual Integrity,” *Washington Law Review*, vol. 79, p. 119, 2004.

[56] W. Zegeye, R. Mangar, J. Qian, V. Morris, M. Khanafer, K. Kornegay, T. J. Pierson, and D. Kotz, “Comparing Smart-Home Devices that Use the Matter Protocol,” in *2025 IEEE 22nd Consumer Communications & Networking Conference (CCNC)*. IEEE, 2025, pp. 1–6.

[57] Connectivity Standards Alliance, “Our Members — Promoters — Participants — Adopters,” https://csa-iot.org/members/, 2025.

[58] R. Mangar, J. Qian, W. Zegeye, A. AlRabah, B. Civjan, S. Sundram, S. Yuan, C. A. Gunter, M. Khanafer, K. Kornegay *et al.*, “Designing and evaluating a testbed for the matter protocol: Insights into user experience,” in *Workshop on Security and Privacy in Standardized IoT (SDIoTSec)*, 2024.

[59] E. Zeng, S. Mare, and F. Roesner, “End User Security and Privacy Concerns with Smart Homes,” in *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 2017, pp. 65–80.

[60] S. Turner and L. M. Tanczer, “In Principle vs In Practice: User, Expert and Policymaker Attitudes Towards the Right to Data Portability in the Internet of Things,” *Computer Law & Security Review*, vol. 52, p. 105912, 2024.

[61] S. Liao, J. Yan, and L. Cheng, “WIP: Hidden hub eavesdropping attack in Matter-enabled smart home systems,” in *Workshop on Security and Privacy in Standardized IoT (SDIoTSec)*, 2024.

[62] H. Wang, Y. Liu, Y. Fang, Z. Jin, Q. Liu, and L. Xing, “WIP: Security vulnerabilities and attack scenarios in smart home with Matter,” in *Workshop on Security and Privacy in Standardized IoT (SDIoTSec)*, 2024.

[63] Y. Liu, J. Yan, S. Liao, L. Cheng, and L. Xing, “WIP: Towards privacy compliance by design in the Matter protocol,” in *Workshop on Security and Privacy in Standardized IoT (SDIoTSec)*, 2025.

[64] Trusted Computing Group, “Design, Implementation, and Usage Principles Version 3.0,” Tech. Rep., 2011.