

# Smart Homes as Digital Ecosystems: Exploring Privacy in IoT Contexts

Sally Bagheri<sup>1,2</sup><sup>a</sup>, Andreas Jacobsson<sup>1,2</sup><sup>b</sup> and Paul Davidsson<sup>1,2</sup><sup>c</sup>  
<sup>1</sup>*Department of Computer Science and Media Technology, Malmö University, Sweden*  
<sup>2</sup>*Internet of Things and People Research Center, Malmö University, Sweden*

**Keywords:** Smart Homes, Internet of Things, Privacy, Digital Ecosystems.


**Abstract:** Although smart homes are tasked with an increasing number of everyday activities to keep users safe, healthy, and entertained, privacy concerns arise due to the large amount of personal data in flux. Privacy is widely acknowledged to be contextually dependent, however, the interrelated stakeholders involved in developing and delivering smart home services – IoT developers, companies, users, and lawmakers, to name a few – might approach the smart home context differently. This paper considers smart homes as digital ecosystems to support a contextual analysis of smart home privacy. A conceptual model and an ecosystem ontology are proposed through design science research methodology to systematize the analyses. Four privacy-oriented scenarios of surveillance in smart homes are discussed to demonstrate the utility of the digital ecosystem approach. The concerns pertain to power dynamics among users such as main users, smart home bystanders, parent-child dynamics, and intimate partner relationships and the responsibility of both companies and public organizations to ensure privacy and the ethical use of IoT devices over time. Continuous evaluation of the approach is encouraged to support the complex challenge of ensuring user privacy in smart homes.


## 1 INTRODUCTION


Internet of things (IoT) devices are increasingly dominating both domestic and public environments for their continued promises to increase comfort, security, and sustainability (Bugeja et al., 2021). Along with their promises, the use of IoT devices poses several challenges related to the large amount of, often personal, data they typically generate, collect, and distribute. In public spaces, some level of privacy might naturally be compromised as the spaces are considered shared and communal. However, in environments generally presumed to be both personal and private – such as the home – these issues are especially concerning when it comes to questioning the expectation of privacy when one is alone. Closing a front door or being physically separated from the public has previously been enough to ensure privacy. Due to pervasive data collection, this understanding of privacy is outdated for IoT contexts as the right to be left alone encompasses all forms of behavioral observation

(Warren & Brandeis, 1989), both from other people and things.

In smart homes, domestic living spaces with people and Internet-connected things (Bugeja et al., 2021), IoT devices often monitor the surroundings ubiquitously as a part of their functionality. This data is central to realizing IoT capabilities such as making smart homes personal, comfortable, safe, and energy-efficient for its users. Just like the system harvesting sunlight, converting it to electricity, and distributing it to power an assortment of appliances enriching our lives, data from smart homes follows a similar pattern. However, unlike solar energy, parts of the data ecosystem are fully digital and not observable in a physical sense. Understanding this digital ecosystem (DE) of users, IoT devices, IoT distributors, and other data stakeholders (such as lawmakers and privacy advocates), as well as the users' concerns about having their private data enable the system, is a cumbersome challenge. Moreover, the diversity of stakeholders involved in delivering IoT services exacerbates the

<sup>a</sup> <https://orcid.org/0009-0009-7387-3367>

<sup>b</sup> <https://orcid.org/0000-0002-8512-2976>

<sup>c</sup> <https://orcid.org/0000-0003-0998-6585>

challenge of understanding the system. For example, IoT users and IoT developers do not commonly have the same level of system expertise and might therefore both understand the system differently as well as approach privacy and its safeguarding differently. The same could be said about IoT developers and law/policymakers as they answer to different stakeholder groups; IoT developers are commonly employed by private companies with economic interests while public servants are responsible for society at large.

Due to the complex challenge of understanding privacy in smart homes, the overarching aim of this paper is to explore the analogy of a DE as a tool to systematize privacy analyses in IoT contexts. Specifically, the guiding question is: how can a smart home be conceptualized as a DE to support the contextual analysis of privacy-related concerns? Currently, no uniform process to model smart homes for privacy analysis has been proposed by the research community nor has systematic processes to present privacy-related research results been introduced. This gap risks valuable insights to be lost due to the failure in compiling and comparing such results. The contribution of this paper is an ontology and conceptual model of a DE to support a systematic approach to analyzing smart homes and their associated privacy concerns.

The next section reviews related work regarding the DE analogy, different dimensions of privacy, and models of smart homes. Subsequently, a method section explains the research process. Lastly, the paper discusses four scenarios of contextually defined privacy concerns and concludes with some directions for future work to continue exploring the DE approach.

## 2 RELATED WORK

A DE can simply be defined as the digital counterpart to natural ecosystems, while a natural ecosystem is energy-centric, a DE is data-centric (Briscoe et al., 2011). DEs have been described as socio-technical systems with “an interdependent group of enterprises, people and/or things that share standardized digital platforms for a mutually beneficial purpose (such as commercial gain, innovation or common interest)” (Rzevski, 2019). The DE is made up of two constituent parts, its species and corresponding environment (Dong et al., 2007), that interact and support each other to sustain the ecosystem over time. The species have been defined as being either biological, digital, or economic (Dong et al., 2007) and can self-organize to sustain their environment (Rzevski, 2019). Additionally, the decentralized nature of the relationships between the species allows the DE to adapt and scale

its size and/or performance. Considering IoT systems as a DE has been suggested before (Rzevski, 2019) and according to existing DE ontologies (Dong et al., 2007), IoT users could be considered as biological species, economic species as the organizations or companies with financial incentives offering IoT services and products, and digital species as all the IoT-related hardware, software, and applications. Examples of digital species could be operating systems, user profiles, APIs, cloud services, as well as IoT hardware, such as sensors, routers, and actuators. Like a DE, the smart home can self-organize to sustain itself over time, and scale towards increased smartness and productivity for its species. An externality of this increased value is the concern for privacy as users’ data fuel the DE.

### 2.1 Privacy in Context

A common definition of privacy is “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” (Westin, 1968). Building upon this definition, privacy can also be defined contextually to consider the prevailing norms of the context (Nissenbaum, 2004). This understanding of privacy goes beyond solely considering data disclosures; a qualitative study looking at smart home devices was able to show how the sense of being watched or observed is at times decoupled from whether data had been generated (Seymour et al., 2020). The feeling of someone else being in the room, such as a voice-controlled Internet-connected assistant, paired with an inability to determine whether disclosures are being made, creates, according to Seymour et al. (2020), a phenomenological privacy concern based on a user’s experience. Meanwhile, purely technological efforts to optimize privacy assurance in smart homes have been introduced and are currently being evaluated (Mocrii et al., 2018). For example, blockchain-based technology (Qashlan et al., 2021) as well as edge computing (Mocrii et al., 2018) have emerged as technologies in support of mitigating data privacy. However, solely ensuring privacy with technological means does not address phenomenological concerns related to IoT usage as it leaves out users’ perceptions and experiences of privacy. To be rendered productive, an approach to analyzing privacy in smart homes might therefore need to include both technical assurances of data privacy, in the sense of information access and exchange, as well as ethical considerations of the social consequences of IoT use that may impact users’ privacy.

## 2.2 Models of Smart Homes

Privacy requirements for IoT systems regard the constraints put on a system to ensure end-user satisfaction, therefore, they need to be considered explicitly (Alhirabi et al., 2021). The main problem lies in the wide range of perspectives that can be taken to safeguard privacy (Alhirabi et al., 2021). Depending on the stakeholder, constraints and priorities might differ seen both to social and technical aspects of the system. In the smart home context alone, IoT devices are being used to offer healthcare, eldercare, and childcare, to name a few, requiring an array of stakeholders to collaborate effectively. The DE analogy has shown promise in eliciting design requirements across stakeholder groups (Koch, 2019) and the smart home has previously been conceptualized as a DE for a variety of purposes, for example, to optimize for energy management (Reinisch et al., 2010), security (Anagnostopoulos et al., 2020), IoT forensics (Grispos et al., 2021), device management (Indrawan et al., 2007), and entertainment (Stanchev et al., 2017). Pillai et al. (2012) developed a model for the technical IoT infrastructure of a smart home and although conceptualizing the smart home as a DE, their model does not include considerations of any social dimensions of privacy or the users' experience. Moreover, models developed for privacy-related research in smart homes vary in detail and perspective, and lack a uniform approach, although most commonly dividing the IoT environments into layers. For example, Bugeja et al. (2021) propose three layers (similar

to Imtiaz et al. (2019)) when discussing privacy placing users in the center with hardware and network layers encompassing it. Systematic approaches to modelling smart homes to explore both social and technical dimensions of user privacy are lacking and deserve further attention.

## 3 METHOD

The research documented in this paper follows the design science research methodology (DSRM) (Peffer et al., 2006). The research process is detailed in Table 1. The aim is to explore the DE analogy and model smart homes as such to support an analysis of privacy-related concerns. Accordingly, two artifacts are proposed: a conceptual model of a DE and an ontology. The research supporting the design of the artifacts is detailed in the appendix<sup>1</sup>. The design objectives (DO1-3) were inferred from the problem statement and following a demonstration of the two artifacts, a descriptive evaluation (Hevner et al., 2008) was conducted by considering four privacy-related scenarios in a hypothetical smart home context. This evaluation method is often deemed suitable when artifacts are both new and unexplored (Hevner et al., 2008), which this work can be considered as. DSRM emphasizes the re-iterative process of designing artifacts (Peffer et al., 2006), therefore, mentions of future research directions are included.

Table 1: The applied DSRM Process (Peffer et al., 2020) with the corresponding sections in the paper.

DSRM Activity	Adaptation for the paper	Section
Identify problem and motivate	Analyzing smart home users' privacy should ideally be done in context. However, seen to its socio-technical nature, a smart home can be modelled in many ways depending on the stakeholder. A DE approach has shown to facilitate discussions across stakeholder groups. Therefore, this paper considers how a smart home be modelled as a DE to support contextual analyses of privacy.	1
Define objectives of a solution	DO1: Is useful to a diverse set of stakeholders. DO2: Reveals privacy concerns contextually. DO3: Includes social and technical considerations of the smart home.	2
Design and development	Based on previous work studying DEs, smart homes, and user privacy, the contribution of this research is in the form of two artifacts: a DE ontology (mainly corresponding with DO1) and a conceptual model (mainly corresponding with DO2, DO3).	3, Appendix
Demonstration	The artifacts are applied to a hypothetical case of a smart home.	Figure 2
Evaluation	Four scenarios of smart home privacy concerns are analyzed.	4, 5
Communication	This work seeks to continue exploring the DE approach by engaging with the wider research community.	

<sup>1</sup> [https://mah365-my.sharepoint.com/:w/g/personal/sally\\_b\\_agheri\\_mau\\_se/ESewZt9MuOFGpwekk-snaRMB9ezTVEzfE-CXi5myh-x4gQ](https://mah365-my.sharepoint.com/:w/g/personal/sally_b_agheri_mau_se/ESewZt9MuOFGpwekk-snaRMB9ezTVEzfE-CXi5myh-x4gQ), accessed 24/01/04.

### 3.1 Digital Ecosystem Ontology

Figure 1 depicts the DE ontology and how a DE is a subclass of ecosystems along with its natural counterpart (Briscoe et al., 2011). In turn, a DE has two constituent parts: species and an environment (Dong et al., 2007). To the three sub-classes of DE species (Dong et al. (2007), a fourth species is added as privacy concerns have shown to differ depending on the nature of the organization (Seymour et al., 2020). Therefore, economic species that are directly involved with offering IoT products and services are distinguished from organizational species such as governmental agencies without financial incentives. The design of the ontology corresponds with DO1 by proposing a uniform approach to modelling DEs based on natural ecosystems, which most have some elementary-level understanding of.

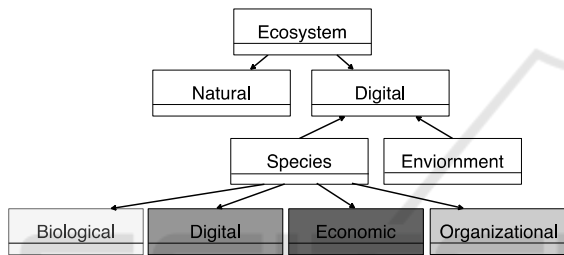


Figure 1: A concept ontology for ecosystems. Downward pointing arrows represent the generic/specific relationship of classes; upward pointing arrows represent part-of relationships (Dong et al., 2007). Species are color-coded to separate them easily.

### 3.2 Conceptual Model

The conceptual model is divided into three layers (Rzevski, 2019; Phillips & Ritala, 2019) to depict the real or social world (structural layer), the digital or virtual world (conceptual layer) and the knowledge base of privacy and ethical concerns (temporal layer). The model’s two top layers mainly correspond with DO3 by considering the social structures of the IoT context and its technical infrastructure respectively. The third layer includes relevant privacy concerns based on the details of the IoT context defined in the two top layers (corresponding with DO2). In this sense, the ontology is used to fill the conceptual model (as demonstrated in Figure 2) to depict the specifics of the context, such as the number of users, IoT devices, and relevant user concerns.

The structural layer defines the relationships between species by considering what is known about the context. The purpose is to reveal how the IoT is being

used, for example, for leisure, comfort, health, security, etc. as well as other social dynamics among the species. Additionally, contractual relationships can be included as some IoT services are subscription-based and might create legal dependencies among species. The purpose of the conceptual layer is to model the flow of user data. Depending on modelling needs and levels of expertise, this layer can take on many forms catering for a diverse set of stakeholders. For this initial iteration of the design process, the conceptual layer is kept relatively simple. The temporal layer could be considered a placeholder for the privacy concerns identified in the context. More research is needed to understand how to systematically document the complexity of preserving privacy in an ever-changing system. For this iteration, Table 2 compiles conceivable change scenarios, categorized according to the species of a DE defined in Figure 1. The change scenarios are based on identified privacy threats related to smart homes (Elvy, 2018; Grispos et al., 2021; Haney & Furman, 2023; Imtiaz et al., 2019; Marky et al., 2021). However, a plenitude of privacy concerns could be considered. Therefore, the idea is less to generate a comprehensive list and more to demonstrate how such concerns can be modelled and analyzed contextually. The selection of change scenarios discussed in the next section regards organizational and biological species.

Table 2: Selection of smart home scenarios.

Specie	Example of change
Economic	- Companies merging, therein, changing the proprietors of data. - A company starts to sell/re-purpose user data to other companies.
Organizational	- If a device happens to record criminal activity. - Increasing number of pre-installed IoT devices in homes.
Biological	- Bystanders entering the home. - Changes in user relationships such as occupants moving in/out.
Digital	- New IoT devices being installed. - Updates to existing IoT device or services changing the flow of data.

## 4 MODELLING SMART HOMES AS DIGITAL ECOSYSTEMS

This section discusses a selection of smart home privacy concerns in a hypothetical smart home context. The details of the context are as follows. Four typical domestic IoT devices (inspired by industry

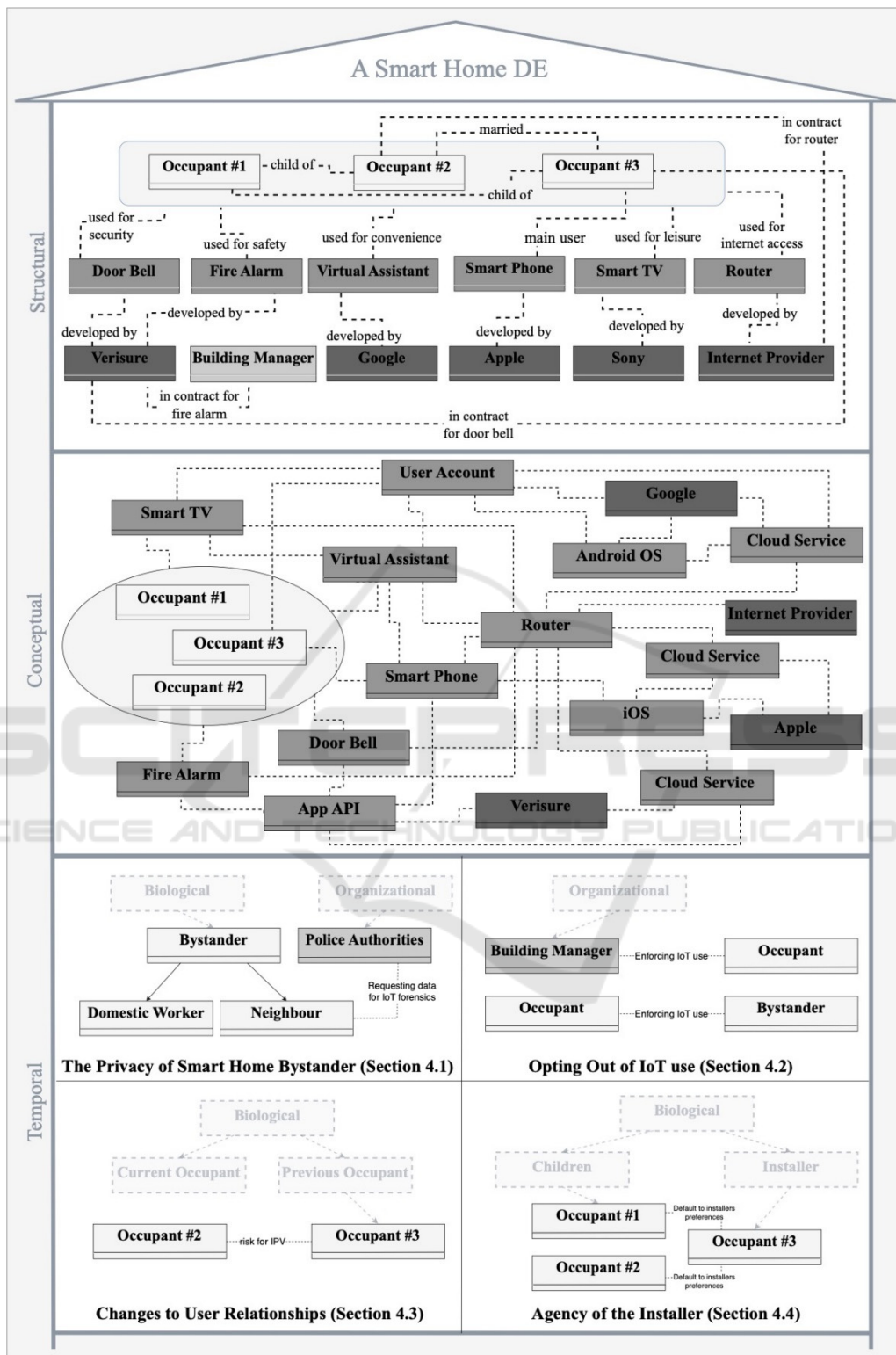


Figure 2: A smart home DE. The structural layer defines the species and their relationships (noted above the dotted lines); the conceptual layer’s dotted lines illustrate the flow of data between the species; the temporal layer illustrates four privacy-related scenarios. Based on the analyzes of each scenario (Section 4), potential sub-classes for future iterations of the DE ontology (Section 5) are denoted in opaque lines. Species are color-coded according to the DE ontology (Figure 1).

websites listing popular home IoT devices<sup>2</sup>) are included: a virtual assistant, Smart TV, smart fire alarm, and smart doorbell. The biological species include two adult occupants and a child occupant. The full conceptual model is depicted in Figure 2 including four privacy concerns derived from Table 2. Although the concerns are supported by previous research and reported cases from the smart home domain, they do not exhaust all the privacy concerns of the context. Instead, the discussion below reveals four potentially unethical smart home scenarios in need of further scrutiny.

#### 4.1 Smart Home Bystanders

As this is a domestic environment, it can be assumed that additional people might occasionally enter the space, for example, as guests. Protecting the privacy of bystanders, defined as users who do not own or directly use the IoT device (Bernd et al., 2020) could partially be considered a technical challenge; depending on the IoT device, data might not be categorized according to users. For example, the virtual assistant in this context (modelled in Figure 2) can differentiate users' voices while the doorbell has no equivalent capability. This could be considered a concern for the occupants as privacy preferences within a household may differ, for example, preferences for children's privacy may differ from adults. However, preserving the privacy of smart home bystanders is of equal importance and in need of ethical consideration. Disputes have emerged in which one neighbor's prerogative to install a smart doorbell conflicted with another's right to privacy causing the first neighbor to take legal action against the second as they attempted to destroy the device in protest to its existence.<sup>3</sup> IoT devices, such as smart doorbells, are intended to generate data from bystanders and could potentially capture illegal activities if it occurs around the house, on the street, or on a neighbor's property. When authorities call upon IoT data to aid in criminal investigations it is referred to as IoT forensics - the use of data from IoT devices as evidence in court proceedings (Grispos et al., 2021). If authorities request data from IoT devices, it can create a trade-off between user privacy and investigation success (Khanpara et al., 2023). More research is needed to consider whether users are obliged to hand over data for IoT forensics and whether it is ethically defensible to subject bystanders, such as neighbors, to non-consensual IoT use.

<sup>2</sup> <https://dgtlinfra.com/internet-of-things-iot-devices/> accessed 24/01/04.

#### 4.2 Opting out of Smart Homes

According to the structural layer of the model in Figure 2, a building manager (organizational species) is in contract with a digital species (fire alarm), not one of the occupants. This can be seen as an example of building managers installing IoT devices and retaining the responsibility for their maintenance. It might be assumed that over time, an increasing number of homes will have IoT devices pre-installed, for example, seen to their capabilities to optimize energy consumption (Reinisch et al., 2010). Both building managers and other stakeholder groups (for example, property developers) could be increasingly involved in the smart home DE potentially making it difficult to live in a home without IoT devices. More attention may need to be paid to include opt-out options or other ways to ensure that a user is not forced to accept IoT devices installed in their home.

Another example of the need for opt-out options is domestic workers, such as cleaners or nannies, as the smart home can at times also be a workplace. In the case of nannies, Bernd et al. (2022) explain how parents might use cameras as a means of control, invading nannies' privacy and even in some cases lead to a reduction in the quality of care for the child. If a domestic worker is surveilled remotely by the homeowners it might be considered unethical if they are not informed or unable to object to such data collection (Bernd et al., 2020). The smart home DE in Figure 2 does not currently have a video-recording IoT device – other than the doorbell which is located outdoors. However, the temporal concern of introducing a new IoT device (Table 2) is relevant to consider as such could occur in the future. In turn, if such a device were installed, domestic workers might need to be included in the DE as biological species to consider their privacy. Whether at work or in one's own home, opting out of smart home systems is a concern in need of further ethical consideration.

#### 4.3 Changes to User Relationships

Of the three occupants living in the smart home, only one is legally in contract for the smart doorbell (see occupant #3 in Figure 2). If that occupant were to move from the home, it would require legal (and perhaps ethical) considerations as to how the privacy of the users still living in the home would be maintained. Hypothetically, if that occupant were to move out of

<sup>3</sup> <https://www.dailymail.co.uk/news/article-10908487/Moment-nightmare-neighbour-tried-destroy-disabled-mans-doorbell-camera-claw-hammer.html> accessed 24/01/04.

the home, they could still have legal access to data from within the smart home. An example demonstrating the risk of this concern is the case of how an estranged spouse who moved from their home maintained remote access to the IoT devices<sup>4</sup>. They were caught eavesdropping on conversations occurring in a home they no longer lived in which points to a larger ethical concern of smart homes: what ultimately became a decisive factor in the case of the eavesdropper were reports of spousal abuse. Technologically facilitated abuse is a growing research area with a sub-domain specifically looking at abuse within the home, or what is referred to as IPV or intimate partner violence (Lopez-Neira et al., 2019). Although previous literature has focused on economic species surveilling users (Zuboff, 2015), IoT devices could potentially be used by biological species to surveil each other, contributing to an increased logic of surveillance (Zuboff, 2015), i.e. how surveillance is increasingly normalized as an unavoidable part of everyday life. Ensuring ethical IoT usage among biological species over time, especially when the relationships between the species change, is a privacy risk of high societal concern.

#### 4.4 Agency of the Installer

Power dynamics among biological species add tensions to privacy as primary users might restrict or control the use and access to IoT devices (Bernd et al., 2022). This can be understood as the agency of the installer (Geeng & Roesner, 2019) which causes all users to default to the settings determined by the installer of the IoT device. In the present scenario, only one occupant's smartphone is connected to some of the IoT devices and can therefore be assumed to be the installer (see occupant #3 in Figure 2). The skewed power dynamic refers to how the installer can potentially abuse their ability to access IoT-generated data thereby violating other users' privacy. As discussed above, examples of this could include the dynamics among occupants (such as in cases of IPV) as well as between occupants and bystanders (such as nannies or neighbors). Additionally, parents surveilling their children to ensure their safety (either remotely or from different parts of the home) could be seen as another example of a privacy concern caused by the agency of the installer. It is worth considering the potential conflict between protecting a child's welfare and the child's right to privacy; at what age is it appropriate for the child to have control over their

data and personal privacy, i.e. to opt out of IoT use? Although the GDPR defines age limitation<sup>5</sup>, the power dynamics between children and adults could impact the exercising of such rights. Special attention should therefore be paid to children in smart homes to explore privacy concerns specific to their user group.

## 5 DISCUSSION AND POINTERS FOR FUTURE WORK

Although not an exhaustive list of concerns, four privacy-related scenarios have been analyzed contextually by conceptualizing a hypothetical smart home as a DE. Corresponding to the activities defined in Table 1, a DE ontology and conceptual model have been designed and applied to support the analyses of the smart home concerns, each revealing notable privacy tensions in need of more research and ethical consideration. Firstly, it is currently dubious what kind of legal responsibility economic species have regarding the data that their IoT devices collect, generate, and distribute. Within IoT forensics, it is not clear whether biological species are required to hand over data if called upon to support criminal investigations (Grispos et al., 2021). This includes data from both within the home and its surroundings which could violate bystanders' right to privacy. Secondly, it is unclear to what extent economic species are required to be proactive and preventative of criminal activity, for example, in the detection of domestic abuse. In situations of IPV, one occupant's right to privacy (perpetrator) could conflict with other occupants' right to safety (victim) which brings into question whether economic species should be required to alert authorities when there are suspicions of abuse. Although that could be considered violating the occupant's privacy, it can also be seen as an ethical responsibility to draw attention to cases of abuse in IPV situations. Thirdly, opt-out options are essential to ensure the ethical adoption of smart homes. Surveillance as an emerging logic might impose IoT use onto users such as bystanders, children, or other smart home occupants. Although there are many valuable applications, opting out of smart environments requires both technical and social considerations of how such privacy preferences can be upheld. Lastly, ensuring children's safety could also motivate high levels of surveillance from parents. A child's right to privacy in smart

<sup>4</sup> <https://www.bbc.com/future/article/20200511-how-smart-home-devices-are-being-used-for-domestic-abuse> accessed 24/01/04.

<sup>5</sup> <https://gdpr.eu/> accessed 24/01/04.

homes needs more research and further ethical consideration as the power dynamics risk making it difficult to ensure such rights.

DSRM emphasizes the reiteration of the design process. Future iterations can therefore consider how the concept ontology could include additional subclasses of biological species such as children and bystanders, to define privacy concerns specific to the different user groups. Adding details to the ontology increases its usefulness to different stakeholder groups to support privacy analyzes. Moreover, developing templates for the layers of the conceptual model could make the modelling process increasingly systematic. For example, previous work on smart home models (Pillai et al., 2012) could be considered to develop device-specific system templates. Based on the digital species defined in the structural layer, templates might aid less tech-savvy stakeholders in modelling the flow of data in the conceptual layer. An alternative avenue for future work is to consider case studies, an empirically strong evaluative method of DSRM artifacts (Hevner et al., 2008). Specific cases, for example, smart homes for health or medical care are encouraged to consider potential changes to privacy preferences when IoT devices are used to facilitate care. Additionally, case studies about specific biological species, for example, children, domestic workers, or bystanders could be conducted to inform the ontology and its sub-classes in productive ways. Continued evaluation in this sense could start building a collection of smart home contexts, conceptualized as DEs, to facilitate an increased understanding of privacy and how it changes based on the details of the context.

## 6 CONCLUSION

Privacy is a central point of concern when dealing with the ethics of smart home environments. Assessing privacy is complex, partly due to the diverse set of stakeholders involved in delivering IoT services and seen to the connotations of smart homes as a particularly private context. The main question for this paper was to investigate how a smart home can be conceptualized as a DE to support the contextual analysis of privacy-related concerns. By following the DSRM process, four privacy-related concerns of a smart home context were discussed and yet, many more remain in need of further consideration. The ubiquity of smart technology and the high level of user acceptance of IoT devices in the home might give the impression of their longevity, however, there is no preeminent understanding of how to address the

privacy concerns introduced by their use. Instead, there is an array of perspectives adhering to different stakeholder groups with different ways to mitigate the unprecedented concern for users' privacy. The contribution of this paper is a DE ontology and conceptual model to support the systematic analyzes of smart home privacy. Although not exhaustive, by applying the DE approach, four privacy-related scenarios have been discussed. The concerns have been analyzed contextually, anchored in a snapshot of a hypothetical smart home constellation, including both technical and social considerations of privacy. However, additional research is needed to empirically validate the DE approach and its utility in supporting contextualized privacy analyzes. By exploring it further, an arsenal of contextually defined user concerns could be compiled to support the determination of similarities, differences, and other nuances to privacy in a wide range of IoT contexts, including but not limited to smart homes.

## REFERENCES

- Alhirabi, N., et al. (2021). Security and privacy requirements for the internet of things: A survey. *ACM Transactions on Internet of Things*, 2(1), 1-37.
- Anagnostopoulos, M., et al. (2020). Tracing your smart-home devices conversations: A real world IoT traffic data-set. *Sensors*, 20(22), 6600.
- Bernd, J., et al. (2022). Balancing power dynamics in smart homes: nannies' perspectives on how cameras reflect and affect relationships. Eighteenth Symposium on Usable Privacy and Security 687-706.
- Bernd, J., et al. (2020). Bystanders' Privacy: The Perspectives of Nannies on Smart Home Surveillance. 10th USENIX Workshop on Free and Open Communications on the Internet.
- Briscoe, G., et al. (2011). Digital ecosystems: Ecosystem-oriented architectures. *Natural Computing*, 10, 1143-1194.
- Bugeja, J., et al. (2021). PRASH: a framework for privacy risk analysis of smart homes. *Sensors*, 21(19), 6399.
- Dong, H., et al. (2007). Ontology-based digital ecosystem conceptual representation. Third International Conference on Autonomic and Autonomous Systems, 42-42. IEEE.
- Elvy, S.-A. (2018). Commodifying consumer data in the era of the internet of things. *BCL Rev.*, 59, 423.
- Geeng, C., & Roesner, F. (2019). Who's in control? Interactions in multi-user smart homes. 2019 CHI Conference on Human Factors in Computing Systems, 1-13.
- Grispos, G., et al. (2021). A digital forensics investigation of a smart scale iot ecosystem. IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications, 710-717.



- Haney, J.M., & Furman, S.M. (2023). User Perceptions and Experiences with Smart Home Updates. *IEEE Symposium on Security and Privacy*, 2867-2884. IEEE.
- Hevner, A.R., et al. (2008). Design science in information systems research. *Management Information Systems Quarterly*, 28(1), 6.
- Imtiaz, S., et al. (2019). On the case of privacy in the IoT ecosystem: A survey. *International conference on internet of things and IEEE green computing and communications and IEEE cyber, physical and social computing and IEEE Smart data*, 1015-1024. IEEE.
- Indrawan, M., et al. (2007). Device Ecology: A micro digital ecosystem. *Inaugural IEEE-IES Digital EcoSystems and Technologies Conference*, 192-197.
- Khanpara, P., et al. (2023). Toward the internet of things forensics: A data analytics perspective. *Security and Privacy*, 6(5), e306.
- Koch, M. (2019). New RE Dimensions for Digital Ecosystems-Initial Results from an Expert Interview Study. *2019 IEEE 27th International Requirements Engineering Conference (RE)*, 398-403. IEEE.
- Lopez-Neira, I., et al. (2019). 'Internet of Things': How abuse is getting smarter. *Safe – The Domestic Abuse Quarterly* 63, 22-26.
- Marky, K., et al. (2021). Roles matter! Understanding differences in the privacy mental models of smart home visitors and residents. *20th International Conference on Mobile and Ubiquitous Multimedia*, 108-122.
- Mocrii, D., et al. (2018). IoT-based smart homes: A review of system architecture, software, communications, privacy and security. *Internet of Things*, 1, 81-98.
- Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev.*, 79, 119.
- Peffer, K., et al. (2006). Design science research process: a model for producing and presenting information systems research. *First International Conference on Design Science Research in Information Systems and Technology*, 83-106.
- Phillips, M.A., & Ritala, P. (2019). A complex adaptive systems agenda for ecosystem research methodology. *Technological Forecasting and Social Change*, 148, 119739.
- Pillai, K., et al. (2012). Hierarchy model to develop and simulate Digital Habitat Ecosystem Architecture. *IEEE Student Conference on Research and Development*, 203-209. IEEE.
- Qashlan, A., et al. (2021). Privacy-preserving mechanism in smart home using blockchain. *IEEE Access*, 9, 103651-103669.
- Reinisch, C., et al. (2010). ThinkHome: A smart home as digital ecosystem. *4th IEEE International Conference on Digital Ecosystems and Technologies*, 256-261. IEEE.
- Rzevski, G. (2019). Intelligent multi-agent platform for designing digital ecosystems. *Industrial Applications of Holonic and Multi-Agent Systems: 9th International Conference*, 29-40. Springer.
- Seymour, W., et al. (2020). Strangers in the room: unpacking perceptions of 'smartness' and related ethical concerns in the home. *ACM Designing Interactive Systems Conference*, 841-854.
- Stanchev, P.L., et al. (2017). Enhanced user experience and behavioral patterns for digital cultural ecosystems. *9th International Conference on Management of Digital EcoSystems*, 287-292.
- Warren, S., & Brandeis, L. (1989). The right to privacy. In *Killing the Messenger: 100 Years of Media Criticism* (pp. 1-21). Columbia University Press.
- Westin, A.F. (1968). Privacy and freedom. *Washington and Lee Law Review*, 25(1), 166.
- Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of information technology*, 30(1), 75-89.