Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Inger Helen Yri

Exploring the design of smart home IoT - How autonomous and free are human users?

Master's thesis in Communication Technology and Digital Security
Supervisor: Katrien De Moor
Co-supervisor: Kaja Fjørtoft Ystgaard
June 2022

NTNU
Norwegian University of
Science and Technology

Inger Helen Yri

Exploring the design of smart home IoT - How autonomous and free are human users?

Master's thesis in Communication Technology and Digital Security
Supervisor: Katrien De Moor
Co-supervisor: Kaja Fjørtoft Ystgaard
June 2022

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

NTNU – Trondheim
Norwegian University of
Science and Technology

Exploring the design of smart home IoT- how autonomous and free are human users?

Inger Helen Yri

Submission date: June 2022
Supervisor: Katrien De Moore, NTNU, IIK
Co-supervisor: Kaja Fjørtoft Ystgaard, NTNU, IIK

Norwegian University of Science and Technology
Department of Information Security and Communication Technology

Title: Stakeholders perception of agency in a Smart Home context
Student: Inger Helen Yri

Problem description:

Internet of Things (IoT) is increasingly becoming more widespread in our daily lives. However, when we let technology into our most personal spaces, such as our homes, the technology must be designed first and foremost with humans in mind. Human agency is defined as: (*"i.e. the ability of individuals to influence and control their motivations, actions, and environment"* [Ban01; KK20]) and is critical for researching, designing, and developing user-centric IoT applications that the user is comfortable owning. Previous research on this topic has found connections between human agency and a positive user experience [KK20; JWJ+12], at the same time, there is scientific evidence that users' can feel tension when it is the device that exercises agency [JWJ+12]. Since smart home technology is becoming more intelligent and can predict our wishes and act independently, addressing human agency in the technical design becomes highly relevant. As a result, there is a growing need to investigate and strike the right balance between human agency and device agency in technical design of the most relevant Smart home use cases to maintain users' needs, well-being, and safety. Is it mainly the commercial and technical incentives and feasibility that determine this balance or is human control, well-being, and safety considered?

To contribute to ongoing research activities and investigate the above balance, I aim to explore stakeholders with a role as the human lead within smart home environment technology design (e.g., policy, industry and academics), to understand the conceptual, and measured/configured notion of human agency in a smart home context (e.g., alarm system, entertainment system or light and temperature regulation). More specifically, this entails mapping out use cases where the balance between human agency and device agency must be carefully considered. Moreover, I intend to use previous research to get an overview of the suggested knowledge needed about IoT devices for users to control their environment and themselves. This insight may be valuable to determining how this balance between human agency and device agency should be operationalized. Finally, insights from the literature will be combined with an interview-based study to collect data and knowledge to outline recommendations for further research on this topic.

Date approved:	2022-02-17
Responsible professor:	Katrien De Moor, IIK
Supervisor(s):	Kaja Fjørtoft Ystgaard, IIK

Abstract

Humans every day lives increasingly involve interaction with intelligent technology. In the last couple of years, humans' most private spaces, namely their homes, have steadily become more technical through the rapid evolution of the smart home Internet of Things. Therefore, it becomes crucial that these devices are designed first and foremost with humans' autonomy and agency in mind to ensure human well-being, control, and safety. As a contribution to ongoing research in this field, this thesis aims to assess if there is an early indication of where and how multi-stakeholder actors, which include policy, government, industry, and academics, in smart home development have autonomy and human agency on their agenda. First, this thesis deep-dives into expert actors' point-of-view. Then, mapping the perceived consequences and use cases, helps identify where the balance between human autonomy and device/technology autonomy needs to be carefully considered to ensure human well-being in smart homes. In order to achieve this goal, users' needs and desires in a smart home context are investigated through a literature review, along with how the expert actors' perspective is illustrated in the literature. Then semi-structured interviews (N=9) with the expert actors were conducted to investigate where we stand today to protect human autonomy and agency.

The main findings from this thesis illustrate that the focus on human autonomy in a technical context is in an early stage. The perceptions among the multi-stakeholder actors vary regarding the interpretation of what the term autonomy means technically and, consequently the extent of having protection of autonomy on the agenda. In order to find a technical solution, consensus on how to interpret autonomy technically can be further developed. This study has identified four consequences, namely manipulation and profiling, possibly accessible health data, decreased privacy, and power relation dis-balance. To minimise these consequences more focus on giving consumers easily understandable information and educational awareness related to technology use can be preventative measures. Furthermore, building meaningful protections for human autonomy early and consistently during the technical development process would greatly improve how to operationalize the concept. However, as this topic is in the early perception stage among all the actors interviewed, future research will be necessary to develop a technical framework that ensures autonomy for smart home users.

Sammendrag

Mennesker sin hverdag involverer i økende grad interaksjon med intelligent teknologi. I løpet av de siste par årene har menneskets mest private rom, nemlig hjemmene deres, stadig blitt mer tekniske gjennom den raske utviklingen av tingenes internett (IoT) for smarthjem. Derfor blir det avgjørende at disse enhetene først og fremst er utformet med menneskets autonomi og handlefrihet (agency) i tankene for å sikre menneskelig velvære, kontroll og sikkerhet. Som et bidrag til pågående forskning på dette feltet, sikter denne oppgaven på å vurdere om det eksisterer en tidlig indikasjon på hvor og hvordan ulike aktører, som inkluderer direktiv, myndighetene, industri og akademikere, i smarthusutvikling har autonomi og menneskelig handlefrihet på deres dagsorden. Først tar denne oppgaven et dypdykk i aktørenes synspunkter. Deretter hjelper kartlegging av de opplevde konsekvensene og brukstilfellene å identifisere hvor balansen mellom menneskelig autonomi og enhet/teknologi autonomi må vurderes nøye for å sikre menneskelig velvære i smarthjem. For å oppnå dette målet er brukernes behov og ønsker i smarthjem kontekst undersøkt gjennom en litteraturgjennomgang, sammen med hvordan aktørenes perspektiv er illustrert i litteraturen. Deretter ble det gjennomført semistrukturerte intervjuer (N=9) med ekspertaktørene for å undersøke hvor de står i dag for å beskytte menneskelig autonomi og handlefrihet.

Hovedfunnene fra denne oppgaven illustrerer at fokuset på menneskelig autonomi i en teknisk kontekst er i en tidlig fase. Oppfatningene blant de ulike aktørene varierer med hensyn til tolkningen av hva begrepet autonomi betyr i en teknisk sammenheng, og følgelig omfanget av å ha beskyttelse av autonomi på dagsorden. For å finne en teknisk løsning, burde konsensus om hvordan man tolker autonomi teknisk videreutvikles. Denne studien har identifisert fire konsekvenser, nemlig manipulasjon og profilering, mulige tilgjengelige helsedata, redusert personvern og ubalanse i maktforhold. For å minimere disse konsekvensene kan mer fokus på å gi forbrukerne lett forståelig informasjon og pedagogisk bevissthet knyttet til teknologibruk være forebyggende tiltak. Videre vil det å bygge meningsfull beskyttelse for menneskelig autonomi tidlig og konsekvent inn i den tekniske utviklingsprosessen forbedre hvordan man operasjonaliserer konseptet. Ettersom dette emnet er i et tidlig persepsjonsstadium blant alle intervjuede aktører, vil fremtidig forskning være nødvendig for å utvikle et teknisk rammeverk som sikrer autonomi for smarthusbrukere.

Preface

This thesis is submitted to the Norwegian University of Science and Technology (NTNU) and concludes my Master of Science (MSc) in Communication Technology and Digital Security at the Department of Information Security and Communication Technology (IIK). The research was carried out between January and June 2022.

There are many to thank for the submission of this thesis. First and foremost, I want to thank my supervisors, Kaja Fjørtoft Ystgaard and Katrien De Moore. I have had the honor to be Kaja's first master's candidate of supervision, and I am beyond overwhelmed by her dedication to the process. Motivation and expertise have been given weekly. And her knowledge in this field has been of tremendous value for this thesis. Katrien is an excellent professor, researcher, and supervisor. She has been available at all times to help me with every challenge throughout this project. It has been a privilege to have been given the opportunity to work with them both.

Nine people have made space in their calendar to contribute with their expertise. I would like to thank them for their patience, time, and last but not least, the very relevant and valuable knowledge on this topic.

Also, a huge thank to my friends and family that have motivated me throughout this semester. It would have been so much harder without you. Last but not least, I would like to thank my parents, Janne Sunde Yri and Kjell Ove Yri. Not only do you perform well beyond what is expected by parents, but with all the love and supporting words, it was always clear to me that you never had a doubt that I would manage this education, even when I sometimes found it hard to believe myself. And for that, I am forever grateful.

Inger Helen Yri
Florø, 16th June 2022

Contents

Appendices

List of Figures

List of Tables

List of Acronyms

AI Artificial intelligence.

GDPR General Data Protection Regulation.

HCI Human-Computer Interaction.

ICT Information and communications technology.

IoT Internet of Things.

NSD Norwegian Centre for Research Data.

NTNU Norwegian University of Science and Technology.

VPN Virtual Private Network.

Chapter 1
Introduction

As digitisation is increasingly taking place in people's everyday lives, it is of tremendous importance that it is designed first and foremost for human users. In the last couple of years, this also includes smart devices in our home, devices that can predict our wishes and act independently, for example, heating systems that can regulate the perfect temperature, and door locks that can automatically open when the user comes home. In other words, centering the design of new services toward humans and human needs becomes even more relevant. However, this also gives rise to concerns that have not been necessary to address before to the same extent. As our environments (e.g., our house, our heating system, our lighting system) become more autonomous, what is needed to be done for the users to still be in sufficient control?

Autonomy is an important component for humans well-being and has for a long time already been important in social and medical science [Nah07; Ski96]. Nevertheless, there are to some degree unknown what position autonomy has in the development of smart home devices. Devices that are developed with the aim of making users' life easier and which are placed in their most private areas, namely their homes. This thesis aims to investigate whether autonomy is on the agenda among the human lead in the smart home industry/development and whether it is considered as important. This also includes to map out what consequences and in which use cases autonomy needs to be carefully considered.

1.1 Context and motivation

The technological shift came almost completely without a warning. In the last 50 years analogue things have gradually become digital, our Nokia 3310 suddenly transformed into an IPhone 6 in the blink of an eye. At least it might feel that way now, when this telephone that once upon a time was used to calling and texting, is today a huge part of our life. We pay our bills on it, navigate, buy buss tickets, use it as our camera and the phone has the pleasure to spend every minute of everyday with us. It is difficult to argue with, that this small computer has made small everyday chores easier and faster. However, the tasks mentioned above also means that this small computer that we bring everywhere contains sensitive and private data, like our location, where we live and where we work. It may contain private photos and maybe also easily accessible personal information. We have our favourite apps on it, that take much of our time. For example, in 2019, the average screen time for 8th grade students in a typical school class in Norway was over three hours a day [Dit19]. And we can only imagine its increase after TikTok became famous. However, recent studies also show that these apps that we like to spend so much time can also be designed in a way that has harmful consequences to human well-being and society [Hon20]. For instance, algorithms are designed for us to constantly want to use the associated application (e.g., Facebook or Snapchat). In fact, the design logic of many mobile applications, in particular in the social media category, resembles the logic of a slot machine in a casino [Rai18].

We are now on the brink of a new shift, this time it includes our most private area, namely our home. IoT and smart homes are now a reality. Almost every thing we own and we can still imagine was once an analogue thing, can now be connected to the internet and communicate with other connected things in a custom made ecosystem in your own home, designed to fit the wishes of its owner. And 5G has just made it much easier [Tel22]. That includes e.g., a refrigerator that recommend dinner recipes, the stereo choosing the background music, the heating system regulating the perfect temperature, and are more energy efficient when nobody is home. In other words it can save us from unnecessary decision making [GC22]. However it is necessary to pay some attention to the Smart Home revolution, for maybe the next time we blink we may not have any choices at all, how autonomous and free are human users then? What happens if we no longer choose our own meals, do not choose the music we listen too, forget to recognise that we are cold because the temperature is always perfect, what happens if we no longer know what we want, because we get used to that every choices is decided for us? We are on a brink of a new era, but this time we know more.

We should therefore use this moment before the shift takes hold to our advantage and design in knowledge-based choices for our future. These devices should be designed in a way that they can fulfil the needs and wishes from their consumers. For that to happen it is necessary for people to get enough knowledge to know what they need and possibly what they might be willing to sacrifice in the process. IoT comes with a lot of possibilities for people and society, and it can in fact be very useful. People struggling with allergies can install air regulations, in order to take measures for a healthier indoor climate. Families can install smart lock systems, so the parents can trust that the door is locked when their kids are the last ones leaving the house. Healthcare devices can be installed in elder people's houses, so they safely can live in their homes for a longer period of time. As we see electricity prices are rising significantly, households can get better control of their power consumption by installing different smart devices. Just to name a few of its advantages. In the aftermath of the Covid-19 pandemic, it is predicted that we will have a noticeable increase in the technological invasion, and IoT will not be an exception [Tel22]. Because the pandemic *"has forced companies to fast-track their digital transformation plans and shift to online commerce to sustain revenues and meet shifting customer demands"*[Tel22, p.2]. This might result in more useful technological components for people and their household. However, it is important to keep in mind that if this happens too fast or in the wrong order it can get fatal consequences. For instance, many people have experienced a loss of control of their personal data thorough social media, as they now are part a business models that use this data for advertisements [Bun22]. And there is a need to remember that this might be fresh in their minds. People and society needs to have trust in technology and smart devices for this technical revolution to be a success, in order to keep developing technological solutions that can be useful for everybody [Ada20]. And if their private life's, human rights and autonomy are challenged too much, many will not be willing to contribute in the technological shift. In other words, this might be a consequence of moving too fast.

The scientific literature contains a lot of research on users privacy and security in a smart home, with obvious reasons [ZMR17; MPK+20; ZGM+19]. However, there is still a lack of understanding when there comes to cognitive, social and psychological effects of digitisation [KK20]. Agency and autonomy have for decades been important in social-psychological science [Nah07]. We have recently throughout the Corona pandemic seen how strong agency and autonomy might be within the worlds population. In the United States of America, the corona measures have almost divided the population [Ant22]. With a long period of obligation of mask usage in a public spaces and at times curfew, have been heavily debated. Many thought it was a necessary to protect people and stop the pandemic, other fined it violation as their right as a human [Shi20]. Also in Norway it has been strong reaction to the corona measures. This is an indication that personal agency and autonomy is important for the population, and should be respected. This still holds for technology. If we install devices that we do not fully understand, that collect personal information that we don't know of, we risk to gradually lose control of our surroundings, and therefore also loose some of or personal autonomy. Further, the loss of ability to act independently and take choices are factors that can be challenged if technology is developed in the wrong way [Hon20]. Recently there are brought concerns that social media might have some of the blame of increase in depression and anxiety among youth [Jul22]. Steinar Krogstad, Professor of Social Medicine at Norwegian

University of Science and Technology (NTNU) suggested in the news article that [1] *"To a large extent, these [social media] companies shape the lives of young people. It is simply billionaires, economists and technologists who control people's behavior for several hours a day. Due to a lack of legislation, the companies have been allowed to regulate themselves."* [Jul22, p.6]

Today we can see that extended digital rights are focused on in European Union. For example through the new European Declaration on Digital Rights and Principles for the Digital Decade [22], which will be explained further in 2.1.2. However there are still not any regulation that directly and fully deals with autonomy technically in Norway. It is therefor of interest to investigate different stakeholder perception of autonomy in the context of Smart home IoT and whether or not they feel a need for this to be regulated in technology.

1.2 Research goal and questions

As smart devices increasingly become a greater part of our everyday life and routines, it is important to address possible challenges to protect humans and society from negative outcomes. The goal of this thesis is to contribute towards understanding how to strike a better balance between what works primarily for human performance and what works primarily for the provider, IoT device or system performance. From the value framework of freedom-based democracies, being in control of oneself and our environment is necessary for the preservation and promotion of human and societal well-being [GBR08; Ski96]. This thesis argues that to achieve an IoT (physical connected environment) that works for humans first and foremost, getting this balance right is a prerequisite to protect user rights, democracy, human safety and freedom, and consequently well-being [GBR08]. (i.e being in control of our-self and our environment) in a rapid growing digitally world.

My contribution is to explore whether achieving primarily human performance (i.e. human and societal well-being), where the necessary protection of human autonomy is of importance, is something that the leading actors in industry, organisations, government, and academics tasked with the digitisation of Norway, as well as regular consumers, have on their agenda. By qualitatively exploring the intention across a broad set of perspectives, I can provide early indications to whether and how the leading actors, organisations and institutions aim to protect human and society first and foremost, in order to achieve a fair balance between human and device/technology agency. Another point of interest is to explore which use cases in a smart home context the experts consider more important in terms of protecting the interests of humans and society primarily, and where is it more suitable for autonomous IoT system/machine to perform control (i.e. how the appropriate balance between human

[1] This quote is translated from Norwegian to English.

and machine autonomy is maintained). Next, these perspectives are compared with the findings from a literature study that investigates where the different expert perspectives (i.e. industry, government, advocacy) currently stand on balancing human control and automation in smart homes. This contribution would help map out where we are today, and if actions must be taken rapidly to ensure that human agency still is maintained in our smart homes. Is it mainly the commercial and technical incentives and feasibility that determine this balance or are human and societal needs and experiences primarily considered? The following research questions are defined and explained as a means to reach the goal.

Research question 1 Are agency and autonomy on the agenda for all of the different stakeholders focused on in this thesis (i.e., Policy, industry, government and academics) with expertise in home environment technology?

We know that autonomy and agency are important for humans in order to feel free to make decisions and be in control [GBR08]. We also have indications that a loss of human agency can emergence in Artificial intelligence (AI) anxiety(i.e., *"the fear of loosing control over AI" [KK22, p.3][JV17]*). However it is also other concerns, both for humans and the society. This digitally evolution is also a cultural shift and there exist a need to align the technological change with the social change [SSA+19]. It is important that trust and proper information is given to the worlds population. So, that people don't go around believing AI will steal their jobs [SSA+19]. Otherwise, there will exist a hostility to smart devices and AI.

Research question 2 What are the most important focus areas/use cases in smart homes where maintenance of human agency should be of highest priority?

As the increase of technology in our household expends, there are important to be aware of possible challenges in different situations. There can be a need to understand which situations it is useful and desired that smart devices can take control over and which use cases it is important that humans stay in control of [JWJ+12; CG16]. However this might be subjective and varies from household to household. Therefor it might not be a specific answer to the question, nevertheless there may be interesting to explore what the experts considers as challenges and possible consequences. This will be evaluated by which challenges and consequences that are mentioned frequently by the expert. And will contribute to where there are important to put the focus in future development and investment in smart home devices.

1.3 Outline

The remainder of this thesis is structured in the following way:

Chapter 2: The thesis background is presented, including relevant research and definition of important terms used through the thesis. The stakeholders different perceptions are presented as well as literature describing the importance of this topic.

Chapter 3: This chapter presents and justifies the methodology used in this thesis. Including limitation and pitfalls as well as analysing methods and tool.

Chapter 4: Present the result and findings from the interviews, and present the material used for answering the research questions.

Chapter 5: Evaluate and discuss the results and set it in a broader context. This chapter also include the answers on the research questions.

Chapter 6: Summarise and conclude on this thesis findings. This chapter also include suggestion to further work on this topic.

Chapter 2 Background

In this section, the literature review that has been used as a basis to substantiate my research, is presented. I explain human agency and device agency in the context of this thesis and the definitions that I have based my research on. Moreover, I look at the rationale for the research design with various stakeholder perspectives and why this brings valuable insight on the issue of agency. Also why I think the focus on different stakeholders perspective of agency can contribute to valuable knowledge on this topic. Finally, previous research about agency in a smart home context are presented.

2.1 Current status from a multi-disciplinary angle

The literature review is framed to reflect the various multi-disciplinary perspectives, with particular emphasis on representing the industry, technology, policy/legal, academic, and consumer views.

In order to explore how IoT technologies protect human well-being and agency, representing a range of original worldviews, the analyses need to compare and deep-dive into various agendas, perceptions, and assessment of implications. It is therefore of interest to dig deeper into various perspectives. In this thesis, these perspectives include:

- Consumer/user
- Legal/ Policy
- Academic
- Industry

The consumer/user perspective is only covered in the literature review, not in the interviews. This is because there are already many studies where consumers' perception is focused on, and the literature review gave a thorough overview of consumers need and wishes in a smart home context. However, there is a need to investigate the other stakeholder perceptions more in-depth.

2.1.1 Consumer/user perspectives

Prior studies have investigated users' perceptions of smart home technology. Below, user concerns, wishes, and claims are presented. Many studies have concluded that users want more transparency and control, especially about their data [EBH+19] and especially regarding how third-party companies handle personal data. [MVS+20]. Others have addressed that several users have expressed *"concerns that the growing dependency on and trust in SH (Smart Home) technologies led to a loss of control and rendered them helpless in case of a technical failure."* [ZGM+19, p.7]. Related to the same issue, researchers have observed that even though users feel a comfort in the automation, automated homes or smart houses can foster a feeling of loss of control [MH12; GC22]. In [ZGM+19] one of the participants had concerns about the Smart House deciding what is best for him/her *“"Of course, it scares me that maybe sometime my house decides what is good for me” (P42)."* [ZGM+19, p.7]. Who in the household controlling the smart devices has also been a topic of investigation. Furszyfer Del Rio in [Fur22] suggests that there are concerns that the smart devices can be the source of conflict in the household. For example, if only one person in the house can and know how to control the smart devices. In other words, several empirical studies aim to map out users' concerns regarding knowledge and control in an IoT and smart home context. Consumers even express concrete desires that can be addressed more directly and can be relevant for stakeholders working on this issue. Some of them are listed below:

- Notification when a device might fail [GC22].
- Easy to handle restart for the hole system [GC22].
- *"Monthly summary about what data has been collected about them"* [EBH+19, p.12].
- Anonymization of the data being collected and without the possibility of trace-back [EBH+19].
- *"Ensure usability and understandability of interfaces with established usability guidelines to enable users to exercise control."* [ZGM+19, p.10].
- Knowledge about who the third-party companies receiving their data are.
- Knowledge about how third-party handles their data [MVS+20].

– More awareness of what is happening around them (i.e., how the system work) [EBH+19].

However, there might also be challenges related to the lack of concern among users. One indication of this is the observation done by Page et al. [PBS+18]. They interviewed 38 young adults and parents about their perceptions of IoT. They found *"that few had a clear understanding of IoT, even among those who had already adopted it"* [PBS+18, p.1]. Another indication here is the so-called privacy paradox. Previous research has stated that people care about their privacy, but at the same time, people frequently appear to overlook privacy [WNC19]. In other words, there seems to be a difference in knowledge and the users' willingness to act to protect their privacy. The result of a survey by The Norwegian Data Protection Authority (DPA) [Dat20] shows that a slightly smaller share is concerned with privacy in 2019 compared to 2014. Also that it is the older participants that care most about privacy.

2.1.2 Legal perspectives

Several attempts to increase the protection of human users and their rights in the IoT context happen through laws and regulations. Even during this thesis's write-up, new EU policies related to protecting users' digital rights have been initiated. The most relevant of them are presented below.

GDPR

When General Data Protection Regulation (GDPR) was implemented in 2018, it in some ways illustrated a much-needed regulated shift in technology. Google, Facebook, etc. have for some time used consumer data to maximize financial profit in their business model [Est17]. With the introduction of GDPR it enabled a legal framework to ensure people and consumers that their data is more carefully handled and, in some ways, give more control back to the consumers. IoT generates a lot of data, and many have predicted that the new IoT decade will provoke a tsunami of data [Collibra; Gua17]. With all this data, GDPR comes in very handy for the users, aiming to protect any directly identifiable personal data. In Norway, the implementation of GDPR has resulted in noticeable changes in the industry [Dat20]. Both private companies, as well as the Norwegian government, had to go through their routine and practices to ensure that their processing of personal data satisfied the requirements of GDPR [Dat20]. In short, this is what GDPR says about the collection of personal data that can be relevant in an IoT context. A summary of the claim states as follows:

Lawfulness, fairness and transparency: *"Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject"* [19, Art.5].

This claim also includes that the subject must consent to the processing of his/her personal data [19].

Information given to individuals: GDPR specifies that people should be informed about: Who the company/organization is, why this company/organization needs this personal data, the categorization of this data, for how long it will be stored, and the legal justification for the processing of this data. It also specifies that the individual should be informed of who else might receive it and if the data will be transferred outside the EU. GDPR further state that this information should be given in *"a concise, transparent, intelligible and easily accessible form, using clear and plain language"* [19, Art.12.1].

European Declaration on Digital Rights and Principles for the Digital Decade

This new declaration puts people's rights at the center and addresses the most relevant digital rights. It is presented as a reference point for businesses, policymakers, and other relevant actors when developing new technology or policy [22] and is therefore also relevant for the purpose of this thesis.

In the declaration, the European Union, commits to [22]:

- *"Strengthening the democratic framework for a digital transformation that benefits everyone"* [22, p.2]

- *"Making sure that technological solutions respect people's rights"* [22, p.3]

- *"Ensuring access to excellent connectivity for everyone, wherever they live and whatever their income"* [22, p.3]

- *"Ensuring transparency about the use of algorithms and artificial intelligence, and that people are empowered and informed when interacting with them."* [22, p.4]

- *"Ensuring that technologies, such as algorithms and artificial intelligence are not used to pre-determine people's choices"* [22, p.4]

- *"Countering and holding accountable those that seek to undermine security online and the integrity of the Europeans' online environment"* [22, p.5]

Digital Service Act and Digital Market Act

There is recently a lot happening in the EU to protect users' digital rights. Among the newest regulations are the Digital Service Act and the Digital Market Act. *"The Digital Services Act and Digital Markets Act aim to create a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses"* [Unib, p.1].

AI act

Within the next few years, the use of AI in smart homes will most likely increase. EU has recently come up with a proposal for an AI regulation named AI act. The regulatory requirements will include a classification of AI systems with different requirements and obligations in a risk-based manner. The main motivation behind this is that today's regulation appears insufficient to handle every risk related to AI technology [Unia]. *"The general objective of the proposed AI act is to ensure the proper functioning of the single market by creating the conditions for the development and use of trustworthy AI systems in the Union."* [Unia, p.3].

Guidelines for private surveillance companies

Security systems are also a part of the IoT and are becoming common in households. There are some laws concerning surveillance companies with important guidelines. These guidelines and recommendation express that the companies *"should publicly affirm their responsibility to respect freedom of expression, privacy, and related human rights and integrate human rights due to diligence processes from the earliest stages of product development and throughout their operations."* [Cou19, V.67.a].

2.1.3 Academic perspectives

Agency in Human-Computer Interaction (HCI) and the context of IoT is also a topic of interest in the academic world. Recently there have been voiced growing concerns related to conflicts between human agency and device agency in smart homes. The scientific papers and their findings concerning these topics will be presented in this section.

We have come to an era where objects and things can exert agency and be agents of actions. Humans that previously exercised direct control over these things are now delegating a certain level of control to their smart devices [KK22]. This delegation leads to possible issues that there has not been a need to address before. Researchers have come a long way to address possible security, and privacy risks within a smart home, even though there still is much work left to explore this field of research. However, there is important to give room for these possible new challenges. As Kang and Kim pointed out in their recent paper; *"although human and machine agency* *can co-exist in human–IoT interactions, it remains unclear how either type of agency exercised in such interactions shapes the psychological, cognitive, and behavioural responses of users."* [KK22, p.1]. There have also been concerns that conflict can evolve when agency within an action is shared. For example, when the device is set to adjust the home temperature based on its owner routine [GC22]. This *"might hinder the user's ability (agency) to produce effects, act, or realise intentions"* [GC22, p.4][AF15]. Agency and autonomy also plays an important role for humans to maintain psychological well-being [Ski96; ZGM+19]. Therefore, there are indications that these possible conflicts needs to be investigated further.

When our things and everyday objects start to act as autonomous agents in a communication chain, that can result in users feeling a social presence as if they where interacting with something social and intelligent (e.g., [Bio06])[KK22]. A social presence that would not exist with an analogue object. Researchers in the HCI field have suggested that social presence is the key psychological mechanism that can explaining why users feel more socially and positively to devices and objects that can exercise their agency [Kim16]. On the other hand, if this social presence gets too strong, users tend to feel discomfort or so-called 'AI anxiety', *which is the fear of losing control over AI* [KK22, p. 3][JV17] .

While some argue that users can feel a loss of control in automated homes [ZGM+19] [GC22], other argue that 's real-time data tracking, analysis and sense-making capabilities gives the users more control over the objects and their environment [KK22]. AI anxiety is also relevant in this context. Previous research has identified various sources of AI anxiety, however, the underlying core source seems to be loss of human agency. [LH20; KK22]. Here it can also be interesting to view it in the context of humans' reaction to devices with agentic capacity. Schmitt [Sch19; Sch20] explains that humans are likely to treat these objects with bias or prejudice. Other *"studies have shown that interactions with an artificial agent that appear highly similar (but not identical) to those with a real human being can threaten a user's sense of human uniqueness and undermine their sense of human identity, giving the user a feeling of eeriness and discomfort toward the agent (e.g., [CPMG19], [SN07]) "* [KK22, p.4].

In order to ensure more human control over technology, there are suggestions that systems should be developed with Human-in-the-loop (HITL), *"which implied supervision from an individual being"*[DDA+20, p.120]. Also, the literature points to an extension from HITL to Society-in-the-Loop (SITL) [Ada20]. SITL that *"does not stop at the individual supervision, but calls into action the wider social context, providing a more inclusive, democratic supervision, avoiding discriminatory algorithms as well"* [DDA+20, p.120-121]. Also, Privacy-by-design (PbD) has been a topic of interest to ensuring more privacy and control for users. Mainly, it illustrates the need to respect users' privacy and include privacy as a default condition in business processes and practices [A C12]. However, others have concerns with illustrating a "quick fix" to the problem. Lindley et al. in [LCC19] suggested that *"ideals like PbD and HCD may coerce technologists to believe that privacy is something that can be ‘achieved’ and a system’s simplicity is analogous to being ‘human-centered"* [LCC19, p.7]. Moreover, Lindley et al. [LCC19] exemplified it with that as every boat, in theory, can sink any system can also be crackable. So instead of assuming a system can be perfectly private by design, they suggest that we rather should embrace these ideals with a healthy scepticism.

2.1.4 Industry perspectives

Technical innovation over the last couple of years paved the way for an increase in the IoT industry. High cost and battery life were once upon a time a challenge now ZigBee has made it possible to produce smart devices with very low-cost and very low-power-consumption [CBGT18]. Also, Z-Wave has played an important role because of the providing of *"reliable, low-latency transmission of small data packets"* and *"with a communication distance that can cover most residence."* [CBGT18, p.2]. Maybe the latest benefits for IoT development are the development and widespread focus on 5G-network. 5G has drastically evolved the mobile networks capacity, and power [Dat20]. It is also notable that another *" major benefit of 5G: The network can be programmed to the needs of various IoT scenarios"* [Tel22, p.4]. Further, the advances of automation, AI and cloud technology are of great value [Tel22]. In other words the available technology make it possible for a rapid advancements in development of the network technology, leading to many business opportunities. The aftermath of the COVID-19 pandemic also plays a key role. *"The COVID-19 pandemic has forced companies to fast-track their digital transformation plans and shift to online commerce to sustain revenues and meet shifting customer demands."* [Tel22, p.2] *"According to The Economist, the pandemic could give way to rapid productivity growth where cloud, big data analytics and IoT are identified as key growth drivers."*[Tel22, p.3][eco20] .

The potential lies not just with the advancement in technology that is readily available but also in addressing some of today’s challenges for the society that may lead to increased demand for IoT services among the population. Maybe most relevant are high electricity prices increase, and ways to save power will probably be of great interest. To put it another way, the significant growth experienced in the IoT industry would not be a surprise.

An important question to ask when development is increasing at a rapid speed: Is the IoT development environment ready? The ENACT project is an EU-funded project and is part of the Horizon 2020 program. *"The ENACT project indicates that there are many feature and functionality gaps in both the applications and* *enablers present in this environment and aims to close some of the significant gaps."* [FSMR21, p.x]. Among some of the challenges are *"the systems' increased complexity, the unpredictability of their environment, as well as the changes in their requirements and infrastructure"*[FSMR21, p.6]. ENACT argue that all of these factors can lead to new threats hindering their trustworthiness. The International Electrotechnical Commission (IEC) report on smart and secure IoT platforms also state that security, trust, privacy and identity management are challenges IoT systems face today [IEC20][FSMR21]. ENACT's approach is to use DevOps to close some gaps and thereby contribute to more trustworthy IoT systems.

That devices from different vendors do not work together has been a problem for consumers and the industry. However, the relatively new standard *Matter* aims to solve this problem. *Matter* is an open-source protocol created by cooperation between a group of leading technology companies, including Amazon, Apple, Google, Samsung SmartThings, and Zigbee Alliance [Row]. *Matter* will make it possible to control the whole smart house through one device, even the devices from different vendors.

Further, Google has recently focused more on achieving human well-being and aim to help users adjust the interaction balance with technology that feels right to them [Gooa]. They propose raising self-awareness and tools that contribute to increased user control, which help put users well-being more on their terms and agenda [Goob]. In other words, there are indications that the industry is starting to implement measures to ensure users' well-being in their products.

2.2 Research gap: finding the right balance between human and device agency

Recent literature suggests that both humans and devices can have the ability to act and make an impact on each other [CSGK17]. Two concepts, human agency and device agency, are relevant to clarify. In this thesis, human and device agency will be used with the definitions below in mind.

Human agency and user agency are often applied interchangeably. In this thesis, human agency will be used. The definition I will base my understanding of human agency on is, in fact, originally defined as user agency. Nevertheless, to emphasize that it is a human user that exercises agency, human agency is used throughout this thesis also to maintain consistency. **Human agency** can be defined as *" the ability of individuals to influence and control their own motivations, actions, and environment"* [KK20, p.4][Ban01]. Then, how can humans know when they exercise agency? *"An agentic person can recognize himself as the originator of his own experiences and actions, not attributing them to an outside source"* [TL20, p.2][MW05].

Device agency is also referred to as machine agency and object agency. Again, many definitions can be used interchangeably, but in a smart home context, device agency is the most appropriate. **Device agency** has been defined as *"the combination of independent abilities the user is willing to attribute to the device"* [TL20, p.1]. However, sometimes the product owner/developers might determine what independent abilities the device should have.

Proxy agency is also a concept that is introduced in the smart home context. Proxy agency can be defined as the concept when the human user delegate *"a certain level of control to objects with a capacity for intelligence"* [KK22, p.1]. In other words proxy agency is the state where human agency and device agency are shared. How to determine who is exercising agency might be an issue. A view on it is that the person or device that initiated an action is the one that exercised agency [TL20].

Coyle et.al [CMK+12] suggested that *"beyond a certain level of assistance by a device, users experience a detectable loss in their sense of agency"* [GC22, p.4][CMK+12]. On the other hand, when the system is designed in a way that it is the user who have given the device instruction to for example change the temperature, a little agency is delegated to the device, but at the same time there are a high degree of human agency and the feeling of control is maintained. When human agency and device agency are adjusted into the 'right' balance, it can positively affect human lives. It can, for example, free the user from some unimportant decision-making [GC22], in such cases as when it can empower the owner of the device by using energy more efficiently and, in some ways, make life more interesting [SF20]. However, as far as I can see, it is still unknown and underinvestigated which specific conditions trigger positive responses and negative responses when interacting with IoT devices [KK22]. Therefore there seems to be a need to define the desired balance between human and device agency. Also, because *"an understanding of user's sense of agency and the agency they give to the device can foster a more empowered relationship between user and device"* [TL20, p.1]. So by investigating the different perceptions of agency and autonomy, we can understand where we are today and what needs to be done to ensure human agency and autonomy in the development of smart home devices. Within the smart home technology space, mapping out the use cases where human agency and autonomy that need to be carefully considered, we can understand how to get closer to calculating the 'right' balance between human agency and device agency.

2.2.1 Autonomy in a psychosocial context

Personal autonomy is an essential part of contemporary human rights [GBR08]. It is important for all humans to feel free to make decisions, and autonomy has for long been central in the field of medical ethics. In medical science, they have a 'Right to self-determination law' also called patient autonomy [Bah21]. That means that it is the patient that decides if he/she should receive the medical care, even though the doctors highly recommend it. In other words, autonomy is such an important psychological component for humans that it has its own law in medicine. However, there are indications that there still is a lack of laws and regulations concerning autonomy directly in a technical context [Kar21].

2.2.2 Agency and autonomy in a technology context

Agency has long been acknowledged as a topic of importance in the HCI community for understating people's interaction with technology [TL20]. Many definitions of agency exist, but their core is the ability to have control of your actions, body, and environment [LCM14]. A more concrete definition in the context of smart home is *"Agency has been defined as the awareness and capacity of an individual (in the context of smart home, a smart device) to initiate causal actions and control their consequence(s)"* [GC22, p.3][Ban01]. In other words, agency is the ability to control your intentions and actions, and act to produce effects [CSGK17]. Another word for the term autonomy is self-determination [Bah21]. There are different definition and subcategories of autonomy, one of them is that *"attitudinal autonomy refers to the cognitive process of choosing and defining a goal"*[NDM01, p.1]. Agency is the most frequently used term in research found related to self-determination in a technical context. However, in social and psychological science, it seems like autonomy is the most used word. Therefore there has been naturally to use both of the terms throughout this thesis, even though autonomy and agency can be seen as two term that describe mostly the same meaning.

2.2.3 What may the loss of agency lead to?

Soraj Hongladarom, in his review of Shoshana Zuboff's book "The age of surveillance capitalism" described that *"Zuboff's main argument throughout the book is that Google's new way of selling their services has resulted in the loss of what she calls "the right to a future tense" for all of its users (Chapter Two, Section VI)"*[Hon20, p.2]. He further emphasizes that this loss becomes a reality when one loose the potential to determine one's future. That this is a result of leaving digital trails in the search engine and giving the algorithms enough content to predict wishes, that can again be used to influence future choices. He explained Zuboff's arguments in the following way: *"Instead of being an autonomous individual who can realize the vision of her own future, the user is trapped in Google's circle of apps and streams of advertisements targeted specifically to her. Her future tense is lost when Google's algorithms already predict all the future she can envision now. When one's future can be accurately predicted, one loses one's autonomy and dignity with it"* [Hon20, p.2]. This illustrates that the potential loss of autonomy already exists on the World

Wide Web. In a smart home context that include more data about routines, and not just words typed into a search engine, this can potently increase this problem if the same approach (i.e., the same business model) is used in smart home devices. In other words personal autonomy might be severely threatened.

It is important to keep in mind that Smart home environments in combination with AI technology represent a cultural shift, where devices and humans must find a way to live together in harmony [SSA+19]. As mentioned earlier, many argue that the solution is to implement human-in-the-loop to achieve this harmony [SSA+19; Ada20]. However, user testing in this context is challenging. The existing testing methodologies do not include testing of a system that changes behaviour based on the routines and knowledge of its users [SSA+19]. That may cause consequences for humans and society, but losing agency in itself may also have fatal consequences. So why should we care?

The Norwegian Data Protection Authority (DPA) published 2020 their result from a survey on a representative of the Norwegian population where they investigated the population's attitudes to privacy and knowledge of the new privacy regulations (GDPR) [Dat20]. The results also show some interesting discoveries from Norwegians' point of view on Smart Home solutions. Half of the respondents were unsure how IoT technology processes and stores the personal data they collect. This uncertainty in the data collection can lead to a change in behaviour. This phenomenon caused by fears of surveillance is called the chilling effect. The survey has discovered that many of the respondents change their behaviour or refrain from doing various activities because of the uncertainty in how companies use their data. [Dat20]

Big data, with all the different types of personal information that may be used can lead to the problem, especially when it is used for analytic matters. For example, when it is used in automated decision making (i.e., *"when decisions about an individual's life are handed to automated processes"*[SSA+19, p.14]). This, among other things, can include a loss of self-determinations and the narrowing of choices [TP12; SSA+19]. This also leads to possibilities for advanced profiling. As the technology comes with many advantages, the advantages might overrule the consequences as described earlier. Findings in [Dat20] illustrate that privacy still is very important for people. However, as the privacy paradox [MVS+20] can be a decisive factor, people might sacrifice their privacy unknowingly.

2.3 How do we solve it?

The paper Smart home technologies in Europe: A critical review of concepts, benefits, risks, and policies [SF20] divided smart homes into five levels. Explanation of the different levels is illustrated in figure 2.1, borrowed from the authors. These levels can be interesting when discussing when user agency is most important. In a level 3 home, devices can be programmed to meet users' need. For example, the users can set the light to turn on when they are supposed to wake up, making this daily task easier for the user. At this point it seems that the agency of the device (e.g. light bulb) only serve humans needs, and as Jia et al. suggested that *"It seems that, as long as the IoT technology serve human needs, interviewees showed consistently positive reactions to popularly available examples or conceptualisations of IoT".* [JWJ+12, p.3]. However, user agency may be even more relevant to protect when we come to level 4 and beyond. When devices start to learn and adopt behaviour from their users to make informed actions, we might have a definition problem of how much agency we want these devices to have. At his level, the devices start adapting to what it thinks the user wants, not necessarily knowing what they truly want [GC22].

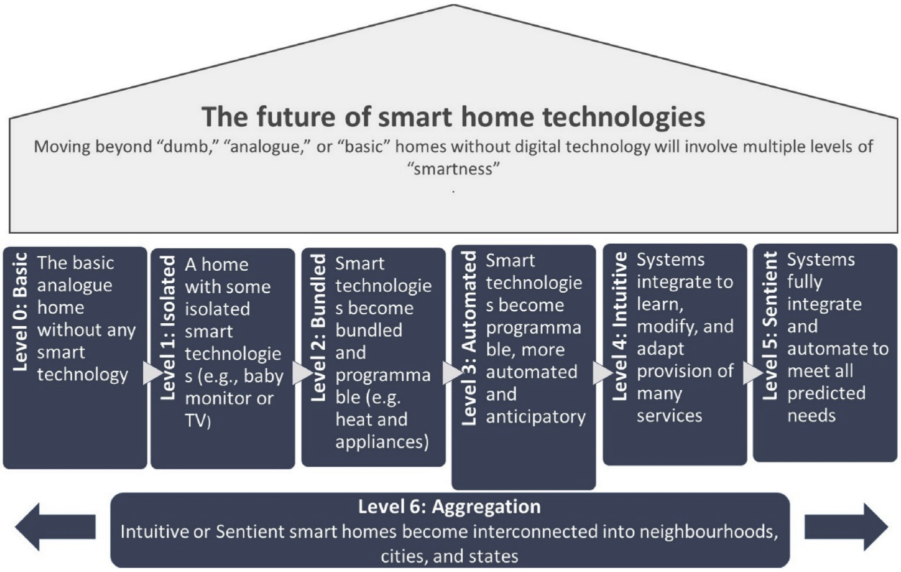
The future of smart home technologies
Moving beyond "dumb," "analogue," or "basic" homes without digital technology will involve multiple levels of "smartness"
Level 0: Basic
The basic analogue home without any smart technology
Level 1: Isolated
A home with some isolated smart technologies (e.g., baby monitor or TV)
Level 2: Bundled
Smart technologies become bundled and programmable (e.g. heat and appliances)
Level 3: Automated
Smart technologies become programmable, more automated and anticipatory
Level 4: Intuitive
Systems integrate to learn, modify, and adapt provision of many services
Level 5: Sentient
Systems fully integrate and automate to meet all predicted needs
Level 6: Aggregation
Intuitive or Sentient smart homes become interconnected into neighbourhoods, cities, and states

Figure 2.1: Different levels of smartness in a smart home context. The illustration is borrowed from the authors of [SF20]

.

The future smart home technologies might predict actions and routines, but what about feelings? Discoveries found in a paper that performed a co-creation workshop with smart home users showed that when there are emotional consequences involved, it is important that the user control is maintained [GC22]. One of the groups in the co-creation workshop concluded that they would not be comfortable with the system taking actions that the humans in the house are usually responsible for, primarily because of the emotional consequences it could lead to. For example, the fear of being replaced or that the system could make the wrong decision that can have negative emotions as an outcome [GC22]. A commonality in the papers that have been reviewed is how human users' private feelings, security, and preservation of private spaces should stay under their control: *"In any case, meaningful human control is a principle that goes beyond any specific protocol; it advocates that humans, not computers and their algorithms, should ultimately remain in control of, and thus be morally responsible for actions mediated by autonomous systems"* [SSA+19, p.5] [CB14] [Svdh18]

Others see concerns in delegating too much to technology without human involvement. C.Stephanidis et al. stated that *"a major concern is that, despite the “intelligence” of the technology and its potential to make automatic inferences and decisions, humans should be kept in the loop through supervisory control and monitoring of intelligent autonomous systems"*[SSA+19, p.5] But how can developers' ensure this level of control for its users? One suggestion is to *"ensure usability and understandability of interfaces with established usability guidelines to enable users to exercise control"* [ZGM+19, p.10]. Another suggestion is that the user should have control in every phase of the system. *"Allow for the user to exercise control in all phases of SH use (before purchase, during configuration and normal operation, and in case of malfunction or threats)"* [ZGM+19, p.10]. Also, in the design phase of smart devices there are human and social aspects that should be considered: *"Designers should think about what things should be connected as well as what things should not"* [JWJ+12, p.3]. However, to get closer to understanding how we can solve this, there is a need for investigating further where we are today, and if maintenance of autonomy and user control is on the agenda for the leading actors in smart home industry. As we have the background material fresh in mind, the next step is to take a closer look at the methodology used in this thesis. The next chapter will explain and justify the methods used for answering the defined research question from section 1.2.

Chapter 3 Methodology

In this chapter, the methodology for this master thesis is explained and justified. The chosen methodology aims to explore experts from different sectors' (i.e., industry, academia, policy makers and government) perception of agency and autonomy in a smart home context and how/if they have it on their agenda. This chapter also introduces The Delphi method as an alternative for a good next step in further research, which is a more complementary method that goes deeper into the investigation, and hopefully might lead to further discoveries.

3.1 Literature review and Research questions

This master thesis is divided in two parts over one year. At the Autumn I took the specialisation project course with its aim to investigate the chosen topic, find relevant sources and making a tentative plan for the master project. This included that the literature review was started, with scoping of the topic and discovering what has been done before and what may need more investigation. The result of this course ended in a Project topic report that was finalised in November 2021 [Yri21]. At the start of the spring semester, the delivered report from the specialisation project was revised and there was a need to scope the problem description even more. Therefore the literature review was continued in order to find more and recent related work. The result from the literature review can be found in chapter 2.

When I had gotten an overview of the topic and problems that still needed exploration, the next step was to define research question. Then the research question from the Project topic report was revisit and specified. The defined research question and its justification is described in 1.2.

3.2 Research Design

In order to choose a research design that fits my project and my research questions, it is important to have an overview of the possible methodologies and methods in order to take an informed choice. The three most used methodology research designs are qualitative research, quantitative research and mixed methods research. Qualitative data consists of non-numerical data, as words, images, sounds etc. [Oat06]. There have a focus on meanings, and situations are seen in the perspective of those involved [Rob11]. Quantitative data is in general data based on numbers. Quantitative research is often done on pre-existing hypothesis, theoretical ideas or concepts and are therefore also used to test qualitative findings [Rob11]. The most generalised difference between a qualitative and quantitative methodology is that: Qualitative research promotes insight and seeks understanding, while quantitative research promotes overview and seeks explanation [Tjo21]. Mixed method is as the word applies, a combination of qualitative and quantitative research [Rob11].

Since I want to explore and gain new knowledge about different stakeholders perception on autonomy and agency, as well as map out the use cases where human agency should be carefully considered, a qualitative methodology is chosen. The main reason for this choice was that I experienced a lot of open ended questions when doing literature searches, which indicates that it is a problem that has not been explored enough in an IoT context. At the same time, a qualitative methodology allowed me to explore if this is a topic of concern in the real world or is something that is already starting to be considered or not. There are indications that there is a need for explorations rather then to concluding on a standard right away and therefore a qualitative methodology was to prefer. However, there are challenges to be aware of when choosing a qualitative methodology. One of them is that the process becomes quite dynamic. As Tjora addressed in [Tjo21], there is a need to take into account that there most likely will occur changes throughout the project. Things may not end up to be as first imagined, we become dependent of the participants' time, and recruitment might take more time then first assumed. Nevertheless, these are risks that sometimes needs to be done to get the answers we want.

There are different methods to choose from in a qualitative methodology, such as observational studies, focus groups, workshops and interviews. My chosen method is expert interviews, also called informant interviews [All17]. The reason for choosing interview is that it let me explore more in-depth as well as gaining insight and knowledge from people with different experience on smart home IoT. By not doing it in a group (e.g., focus group), I can focus on one point of view at the time. This set-up will also hopefully contribute to the participants feeling able to fully speak their mind, without interruption. I also did not want to shape the answers, that might be a consequence if for example a quantitative methodology with a survey was chosen. However it is notable that time limit of the project as well as available resources contributed to the choice. It became natural to me to investigate the expert view, since the literature review gave me an insight on users perceptions of smart homes. Therefore I found it valuable to see how the industry standards in development of smart home devices are, and if there are done attempts to meet the requirements of the users. It is also of value to interview different stakeholders to get a wider view on how we do it today and if there are disagreements on how it should be done. Because in my opinion, cooperation between the chosen stakeholders (i.e., industry, academic, policy and government) is of great important to ensure human-centric smart home devices that ensure maintenance of human agency.

There are three types of interviews - Structured, Semi-structured and Unstructured interviews [Oat06]. They are characterised by the degree to which they are pre-planned. For the purpose of answering the research questions defined, semi-structured interviews are the chosen interview method. The reason for this is that there are experts in different professions, and an interest to ask questions related to their specific expertise. In other words, even tough the essence and the goal for each interview is the same, some of the questions vary depending on who the interviewee is. Then there is done an attempt to cover their whole expertise and hopefully get an indication of the point of view of the perspective they represent. Because of this, fully structured interviews were excluded, as the latter often have a similar structured for each interview where the questions are pre-determined and asked in every interview [Oat06]. Since I want to get answers on several different topics, it most likely would be necessary that the interview is pointed in the 'right' direction. And therefore there are a a necessity to plan some of the questions in advance, therefore a totally unstructured interview is also excluded because there is a need of some pre-planning. The conclusion is that for this thesis specific problem description, semi-structured interviews is seen as the best fit. Also because it lets me pre-plan the structure, but also gives the interviewee room for reflection.

The Delphi method was also considered as a method. *"The Delphi method is an iterative process to collect and distill the anonymous judgments of experts using a series of data collection and analysis techniques interspersed with feedback"* [JTK07, p.1]. The process is often repeated until consensus is reached [JTK07]. On this topic the method is valuable for gaining consensus between the relevant stakeholders in a preferable why and for development of a framework that ensures human-centred Smart Home devices where agency and autonomy is maintained. However there was concluded that there was a need for some explorations beforehand, also time and resources was a challenge to implement this method into this thesis. Nevertheless this thesis argue that it is a great next step for further research on the topic.

The chosen methodology for this thesis is therefore a combination of a literature review and semi-structured expert interviews. The literature review will work as the conceptual framework (i.e how I think about the topic and structure the research process [Oat06]) of the thesis. The literature review was also useful to pinpoint the problem description and get an overview of what has been done before, and what is still left to be addressed [Oat06]. The related work from the literature review will also be used as comparison when analysing the result from the experts. It will be of interest to see whether the perceptions from the different stakeholders that are illustrated in the literature review are aligned with the experts that I am interviewing or whether different views are illustrated. Since some qualitative research previously already has been conducted to map out users wishes and concerns when it comes to smart home, it will be interesting to see if these wishes are met in the design. As well as see how they work to solve the users concern in the design process of their products. Therefore a semi-structured approach will be useful to discover comparable patterns, as well as get a deep dive into different perspectives.

As to the structure of the interview, a focused interview was chosen. Focused interview are interviews that are limited to a specific topic, and do not need the same duration as for in-depth interviews that traditionally lasts an hour or more [Tjo21]. The reason behind this choice is since I am interviewing experts in the field of Smart home IoT, and since the interview most likely will happen in their work day, the duration has to be as limited as possible. Since there probably is difficult on both sides to get enough time dedicated to do an in-depth interview. Therefore a focus interviews with the duration from approximately 30 minutes was chosen.

3.3 Interview Guide

Then the Interview guide must be made, so that the relevant topics are covered in the interview. The Interview guide was designed with help from examples from C. Robson's book [Rob11] and the use of topics was inspiration gained form Tjora's book [Tjo21]. For compiling the interview guide it important to know how to structure the questions, to get the relevant answer. Also, since I am exploring how the process is today, it is important to ask open-ended question and let the expert reflect. In that way I will know where to put the focus for the rest of the interview. The interview guide can be found in the Appendix. Appendix D contains the interview guide used for the Norwegian-speaking participants and Appendix E was used for the English-speaking participants.

The general structure started with an introduction part where I introduced myself and the purpose of the conversation. Then I asked a warm-up question where I let the interviewee explain briefly what they specifically have worked on related to smart home. This is of value so that I can use that to ask more specific question and get the most out of their expertise. In the general questions there are of great importance to ask open-ended question since I want to explore whether agency and autonomy are on their agenda, therefore I will try to make them mention it, before I ask them about it.

There are also different focus areas for the four different expert views. Even tough the focus holds for all of the interviews (i.e explore different stakeholders perception of agency/autonomy in the context of smart home IoT), there are different insights to get out of each expert group. I have therefore defined general questions for all the interviewees as well as specific questions for each expert group. Beside this, I have defined four main-topics that there will be done an attempt to hold for all of the interviews. They are as follows:

- Advantages and disadvantages with smart IoT
- Main goal or purpose of smart/IoT or their product (if industry/government)
- The design process and the focus of autonomy/agency
- Consequence and risk for people and society

The design process and the focus of autonomy/agency section includes questions that might only be relevant for the industry participants (i.e., about practises as user testing and what standards they use). However, that section also includes general questions that was asked to everybody. Even tough the interview guide is of great value to get a structure of the interview, as well as guarantee that the questions needed are conducted, it is also important to mention that its main purpose is to work as a guidance in the interviews. If concerns that are not thought of beforehand are mentioned by the expert, it is important to ask follow up questions at that topic as well. In other words, the guide will most likely be different for each interview since it is difficult to fully plan the conversation beforehand. However, it is vital that it is followed in a way that it gives enough insight, in order to get new knowledge to answer the defined research questions. It is also important to try to 'stop by' each section as describe above, since this will be of value for the data analysis phase.

3.4 Selection criteria

As a means to answer the defined research questions it is of great important to ask the right questions to a carefully considered audience. The selection criteria for recruitment for interview are presented and the reasons behind the choices are explained. The expert panel consist of four stakeholder perspectives, where in this setting expert is defined as people with academic knowledge, policy knowledge or work related knowledge for Smart home IoT solutions. Besides the four stakeholders focused on in the interview part, the consumer perspective has also been investigated in the literature review, and has been important to know where to put the focus in the interview. The expert perspectives and the reason behind the selection is explained more below.

- Expert(s) with policy perspective
- Experts with industry perspective
- Experts with academic perspective
- Experts with governmental perspective

The reasons behind the specific grouping of stakeholders are illustrated in the figure 3.1. All of them have an interest in the end user, however they might have different interest/views on the situation. To meet the users wishes and concerns, this thesis argues that ideally cooperation and dialogue have to be maintained between each stakeholder group. Therefore there is of interest to explore their perception of this topic. Below are each expert group explained in more detail.

The Policy perspective: This group includes people that work with human rights/ and well-being of consumers in a technical context. This group's insight will give this thesis an overview of which regulation companies on the Norwegian Smart Home markets is obligated to follow, but will also allow to get an overview of which might be missing to ensure autonomy and agency in the products. Hopefully, the interviewee will also have insight on how regulations in this field work in practice. It is of value to explore if agency and autonomy is on the agenda for policymakers and whether they believe today's regulations succeed in protecting users' autonomy.

The industry perspective: This group includes people working in the industry. That is people with a job in companies, small as big that work with smart home or IoT solutions. These insights will give an overview of how the process goes from design to the end product. More specifically, how the product is developed to ensure that the regulations are followed and how they ensure the well being of the humans in communication with their product. In this thesis, the focus will be on the user testing procedures as well as how they evaluate that the regulations are met. One other reason for why this perspective is beneficial is to check whether they think today's regulation is necessary, whether they see a need for more regulations, or whether they think that humans well-being already is maintained in the design/user testing process. This information is necessary to continue a a good collaboration with the government and policymakers.

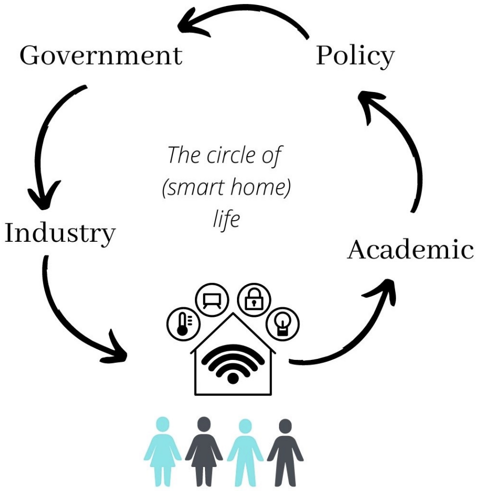

Figure 3.1: The figure aims to illustrates that each stakeholder group has an impact on the end product and therefore also on the user. Therefore, this thesis argues that cooperation between all the stakeholders is necessary for the development of smart devices that first and foremost meet users' needs and protect their well-being. They might have a different point of view on smart device development, however, an interest in a trusting relationship with the users is most likely a common goal.

The government perspective: This group includes people working on developing digital solutions in the government sector. In the Norwegian democracy, it is important that the government works for the general populations well-being and security. This is an important factor for why the Norwegian government has a large share of trust among the Norwegian population [Dat20]. This still holds for technological solutions. There might therefore be a distinction between the technical solution developed by the government for the people compared to solution developed by the industry for the free marked. Therefore there are also of value to investigate the development process in government sector at the same rate as the industry.

The Academic perspective: This group includes people in academia, that have a focus area within smart IoT and/or human-centred design. Both academics that have years of experience in the field of Smart home IoT/ HCI/ Automation but also PHD/ other candidate that have a good insight in the recent literature. And therefore researcher that has seen the trends through time, as well as expert with new insights that can be able to pinpoint future challenges. Here I also had a focus on diversity on focus areas. For example one of the participants focused on privacy awareness and privacy challenges for consumers of IoT devices and another focused on challenges related to the software engineering.

Exclusion criteria: The following exclusion criteria were used:

-Experts that do not have opportunity for decision making in their field, are therefore not the most relevant when recruiting people for the industry perspective. That can be a development consultant who has just done some modification on the product, and who hasn't been part of the whole project. And because of that might not have a good enough overview of the process.

- Experts who have too much a commercial view. They might not be able to tell the whole truth because that might harm their product. Hopefully the information about anonymization will help.

- Experts who only work on advancing technical challenges and don't have insight on user involvement.

3.5 Recruitment strategy

The next step is to know where to contact them. If it is difficult to find their contact information (mail, phonenumer), Linkedin was used first. Linkedin was a good platform when contacting leaders and company owner (I.e., very busy people) since one can assume that their inbox is very full already. If it after the first message is difficult to get a response, I consider calling them or send a message on their phone to let them know that I have sent them a mail with more information. Here, vocabulary and formulation will be important since hacking attempts are a topic of concern right now. However, the use of messages and calls did not become necessary. Snowball sampling [Oat06] was in some cases used to find more experts.

3.6 Data collection and Privacy

It has been of great importance to me to protect the privacy of the participants. This so the expert can feel that they can speak their mind without any consequences for them or the company they represent. The projects has been approved by Norwegian Centre for Research Data (NSD). NSD has been commissioned by NTNU to investigate that the personal information collected in this project is in accordance with the privacy regulations. The approval on the NSD application can be found in Appendix A. All of the participants were also informed about this and received a consent form with more information that they had to sign. The Norwegian consent form can be found in Appendix B, and the English consent form can be found in Appendix C.

The interview was held over zoom with Feide log in. Virtual Private Network (VPN) was also always on to ensure encrypted communication. The recordings was then stored on a cloud supported by NTNU and deleted when no longer needed. In the transcription all the identifiable information about the participants was removed.

3.7 Data processing and analysing

3.7.1 Transcribing

Since the interviews were video recorded, there is a need for transcribing the interviews. An effort was done to finish transcribing one interview before the next one, so that I had the possibility to learn from eventual mistakes and more easily could improve the interview guide. My routine for transcribing the interview was first to use the Microsoft Word recording function, as I experienced that it was quite accurate. Then I went through the recording myself, paused, went back, and made the necessary changes. If there was hesitation, I made sure to include this in the transcription. Since struggling to find words can indicate an uncertainty and it is difficult to know if this is of value for the analysis at this point [Tjo21]. Therefore, there are better to include it and rather remove it later. Then I went through it a last time to check that the transcription was a written copy of the recording. I also had prepared an Excel sheet with the main topics from the interview guide. When a topic of interest was mentioned in the interview, it was pasted into the Excel sheet. The purpose with this was to test if Excel could be an appropriate tool for structuring and analysing the collected data. After the first two interviews it was very clear that there was too extensive amount of data, and a different plan needed to be calculated. The excerpt used in Chapter 4 was later translated to English so that no-Norwegian speakers also can understand them. There was a great effort to ensure that the same meaning was visible after translation. Therefore, they were generally directly translated.

3.7.2 Coding

Nvivo[1] was chosen as a coding and analysis tool. The goal with coding is as Tjora mentions in [Tjo21] to extract the essence from the empirical data, to reduce the amount of data and last but not least to facilitate idea generation based on details in the data. By using an inductive empirical coding approach, the influence from own expectations and assumptions may be reduced [Tjo21]. Therefore, this coding approach was used. The purpose is to generate codes that are as close to the participation statements as possible, then the codes later can work as bullet points to attach the information to. For transcription by transcription and line by line, codes were generated with information that may be useful to answer the defined research

[1] https://qsrinternational.com/nvivo

question. If there wasn't already a code to attach the statement to, a new one was generated. In the end, 175 codes was generated.

3.7.3 Categorisation and thematization

The final amount of code is quite overwhelming and too unstructured to analyse. Therefore codes with a thematic relationship were categorised together, also codes that were irrelevant for answering the research questions was separated out. At the end, codes were categorised into 8 categories, namely: Autonomy, Benefits, Challenges, Development Process, Regulations, Solutions and Trust. These categories are used to formulate themes that will be presented in the result chapter and later discussed in the discussion chapter. The categories was used to made the following themes:

Theme	**Categories**
Perception of Autonomy	Autonomy
Autonomy on the agenda	Autonomy, Development process
Use cases that need more focus	Consequences, Regulation, Trust, Challenges
Suggested solutions	Solutions, Regulations, Benefits

Table 3.1: An overview of themes that laid the foundation for the analyzation presented in chapter 4.

3.8 Limitations and pitfalls

There are some pitfalls of choosing interviews as the main data collection method. One of the major ones is that this makes me dependent on other people's time and availability. This also becomes very relevant since I aim to interview experts and therefore also people that have limited space in their calendars. Therefore the recruitment strategy has been important, and a great amount of time has been used to design the recruitment email. This use of time later turned out to be a success since most of the recruited participants made themselves available.

Another pitfall is the sample size. Since interview is time-consuming, there was only time to interview nine expert. Four from the industry perspective, three academics, one from the policy perspective and one with a government perspective. To say that these nine people represent all of the four perspectives would be a rough generalisation. I will therefore be aware of this when presenting the result and be careful for concluding on a general basis. However it provides a starting point for finding out where we stand today and what should be done in the future.

Because there still was a pandemic when the methodology was planed, there was naturally to choose digital interviews. That brought some advantages, such as it became easier to recruit since nobody had to travel for the interview, and it also seemed like it was preferred by the experts. Nevertheless it also brought some challenges. The most obvious was technical issues. This happened three times. The first time I lost my internet connection that lead to some minutes lost from the interview and also a break in the interview flow. The two next times, the participants had difficulties with attending the zoom link. One of them made more time in their schedule to finish the interview as planed, the other had to reach a meeting and the interview therefore became a little shorted. These challenged brought with some stress for me as an interviewer, but it seemed like technical challenges was nothing new for the expert after two years of home office, so luckily it did not affect the interviews critically. Another pitfall from technical interviews is that interaction digitally may not be fully comparable to a conversation where both are in the same room. It might be difficult to discover body language and therefore also misunderstand some of the answers. As video recording was used in seven of the nine interviews, it did not seemed to be that much of a challenge. But because of the technical problems mentioned above two of the interviews was hold of camera, then it was important for me to ask follow up question if I was uncertain if I understood the answers correctly.

3.8.1 Bias

This project, as many others contains the possibility for bias. The reason for wanting to investigate this topic further is my perception that this is not covered enough today, therefore I obviously had a critical view on the subject beforehand. However as I aim to investigate how it is today, it is important that I have an open mined to the topic. Therefore there has been done some measures to try to avoid as much bias as possible. Since I recruited the participant systematically myself instead of for example a random sample of people, this may lead to bias. Nevertheless it has been important to me to interview almost the same amount from the academic view and the industry view. Also to have a diversity in the different categories. From the industry I both had participants from small companies as well as well-established companies. And for the academics I recruited people with years of experience as well as younger participants. One had the focus area on protecting privacy of users, and another on more the software engineering side of smart home. Then I hopefully could get a broader view on the topic. Another measurement was to be open about this to my supervisors, then risk of bias would be easier recognised. In the interview guide I also made sure to included questions about benefits and not only challenges. Also when analysing the transcription I choose a inductive empirical coding approach, since this may help reduce the influence from own expectations and assumptions [Tjo21]. I have talked a lot about this topic with friends that I know are very enthusiastic for smart home technology and tried as much as possible to have an open mind. Although it is difficult to remove all bias out from the thesis, I have done all I can think of to minimise it.

3.8.2 Lessons learned

As this is my first time collection interview for a research project, there are naturally some lessons learned. Even tough I made sure to read up on several do's and don'ts in advances, I experienced that it was easier said then done in practice. For example I had understood that it was important to listen more then I speak and ask short and informed question. I discovered when transcribing the first interview that I asked very long follow up questions, since then I did not have the interview guide to follow. That resulted in that the interviewee had do ask what the question really was, and unnecessary time was spent on it. Also I definitely listen more then I spoke, but it was difficult not too interact with personal meanings in the conversation. Luckily the interviewee was very professional and it was clear that this did not effect the answers. Therefor is was also of great value to transcribe the first interview before doing the next one, since I then became aware of this and made sure to ask shorter question the next time, and only listened and rather ask curious questions when interesting topics was mentioned.

How autonomy was introduced in the interviews should be done more open and consistent in all the interviews. Also to put in more effort to make the participant directly define the word autonomy in a technical context. As this was discovered a bit late in the interview process, there was rather a need to investigate their perception of autonomy in how they talked about it. For example if they talked about control over personal data, or if they mentioned a trusting relationship between the consumer and company as an important factor etc. So, if I had the possibility to do this again, I would have introduced autonomy more consistently, as well as make the participants define the term directly.

Not asking leading questions also proved to be difficult. Even though this did not happen often, there was some cases where it happened. Here I had the great advantage with interviewing professional expert that had strong opinions on many of the topics, they maid sure to speak their mind even tough the questions could have been formulated better. When I became aware of this, I made sure to prepare some new questions about the topics where it happened for the next interview, too reduce the occurrence. However this was also something I had in mined when analysing the transcription, to make sure that the statement included in the analysis was valid. This also made it clear that it was an advantage to do two test interview before the first expert interview was collected, so the most critically mistakes was discovered then. All in all it was a great experience too see that I evolved in the process, and the interviews become gradually smoother.

Chapter 4 Results

This chapter present the findings from the nine interviews conducted as part of this thesis work. In 4.1 the experts perception of agency and autonomy is presented. 4.2 have the focus on if the experts have agency and autonomy on the agenda or if they see the need for this focus in smart home design and development. These sections aim to present the data for answering RQ1. In 4.3 several concerns from the experts are presented, and concerns mentioned by multiple participants set the foundation for use cases that need more consideration in the future. Finally, sub section 4.4 represent the participants' advice to possible solutions to the challenges mention in 4.3. These two subsections present the data for answering RQ2. Some of the relevant excerpts from the transcriptions can be found in tables through this section when there is a need to illustrate more then two perceptions, aiming to make the result easier to understand.

The final amount of interviews was in total nine. Of these, four people came from industry, three experts are from academia, one is from a governmental sector and finally, one works with policy related to digitalization and technology. Within the industry three different companies are represented, in other words there are two interviews from the same company.

4.1 RQ1: Perception of Agency and Autonomy

It was investigated by means of several general question whether agency and autonomy were mention first by the expert. By these answers, an attempt was done to prone the follow up question to talk about agency and autonomy in its meaning (i.e., the essence of agency and autonomy). Several of the participant mentioned control, either as a benefit or a challenge. Almost everybody mentioned increased control over your house and environment as a benefit. However, in all of the nine interviews, it was a necessary to introduce the concept. This usually happened when there was 15-10 minutes left of the expected time. It varied how this was presented, according to

Participants	Profession	Gender	Duration	Language
P1 (E1)	Policy	Female	30.33 min	Norwegian
G1 (E4)	Governmental sector	Male	28.37 min	Norwegian
A1 (E3)	Academic	Male	39.48 min	Norwegian
A2 (E6)	Academic	Female	32.11 min	English
A3 (E8)	Academic	Male	30.16 min	English
I1 (E2)	Industry	Male	26.56 min	Norwegian
I2 (E5)	Industry	Male	21.47 min	Norwegian
I3 (E7)	Industry	Male	33.54 min	Norwegian
I4 (E9)	Industry	Male	29.06 min	Norwegian

Table 4.1: An overview of the participants, their profession, gender, interview length, and the language used in the interview.

what was natural in the conversation. A repeater was: *As recently seen in literature, autonomy has started to be mentioned a lot with technology. Do you have knowledge of that concept?.* Since I did not manage to fiend a Norwegian word for agency, I concluded that autonomy covered the essence of what I wanted to investigate. However, I introduced the term to the two first academics, they were both familiar with the term autonomy, but they had not seen the term agency before. In most of the interviews, unfortunately I did not manage to make them directly define the term autonomy in a technical setting. Although what they first mentioned as examples and where they put the focus can say a lot about what they put in the word. Figure 4.1 illustrates the amount of participants that stated that they had knowledge about autonomy and figure 4.2 illustrates the participants perceptions of autonomy based on the conversation around it in a smart home context. If they first answered no to the question about knowledge to autonomy, it is further discussed and explained, and if they still did not have a perception of it, they was moved to the 'no' category. The participants' perception of autonomy is presented in this section.

Eight out of nine participants had a perception of autonomy in an technical context as illustrated in 4.1. **I1** answered "no" when he was asked if he had knowledge about the term autonomy in an technical context. Then the term was explained, but he did not change the answer when asked if autonomy was on the agenda now or if he saw some challenges with it in his work. When asked if he saw any problem with a possible loss of personal autonomy, he answered: *"No I think those who are growing up now grew up with such a healthy scepticism of technology so so I think it's more about informing and the people are aware".*

The rest of the participants' first statements around autonomy are categorised

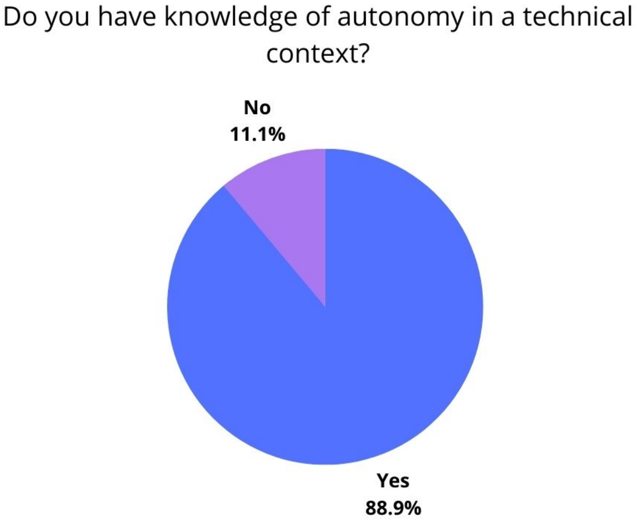

Figure 4.1: Eight out of nine had a perception of autonomy in an technical context. I1 answered no to the questioned. *The illustration is made with the tool and website canva.com*

into six themes, namely: Control, Decision makers, Mastery, User Protection, Trust and User dependent as illustrated in the figure 4.2. A little more information about in which context they put the theme can be found in the boxes to the right in the figure. Five participants mentioned control, among them participant **I4**, who also focused on mastery and **A3** also focused on user dependent, the same as **A1**. The two others had individual perceptions. The figure therefore also illustrates that there are different perception of autonomy among the different stakeholders, also among the stakeholders that represented the same group. Since there are some differences among the participants, we will go more in detail about their statements below.

Control was the most repeated topic. However, it varies in what the focus around control was. The statements concerning control can be found in table 4.2. **P1** focused on that uncertainty about how things work and what the data is used for can feel like a loss of control and lead to change in behaviour. **G1** first mentioned that there are benefits with an autonomous house. However, there are possibilities that someone can take control of the house, and that this is a scary thought and a threat. **A3** focused on that the users should have control of the whole system, thereby also about what data is collected which was also **A2's** focus area. **I4** explained that the solutions should help to give consumers control over for example their smart home, and therefore that it should be understandable and predictable what happens.

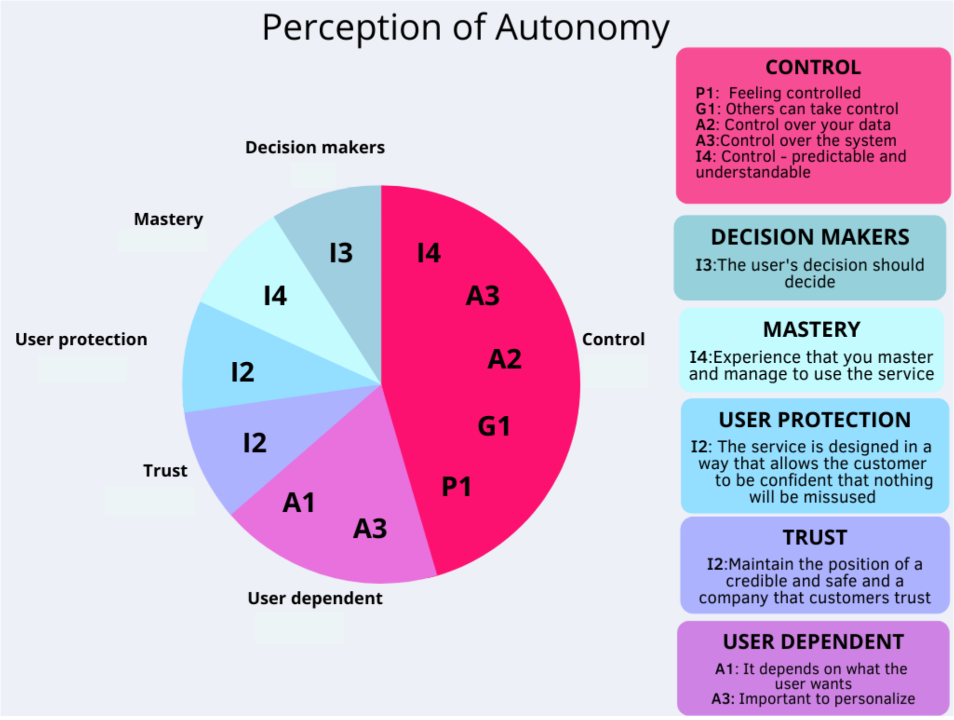

Figure 4.2: The figure include an overview of the participants statements when they where asked about autonomy in the context of smart house. The thematization is based on how the participant reflected around autonomy, and where they put the focus. Some of the participants (i.e., I2, I4 and A3) focused on more then one main theme, therefore they are connected to more then one theme in the illustration. Five participants talked about control. I4 focused both on control and mastery and A3 on control and user dependent. The two others had an individual perception as illustrated. *The illustration is made with the tool and website canva.com*

A1 first statements around autonomy was themed as user deepened, this because he based he's thought on autonomy in a smart home context around the fact that it depends on what the user wants. He also stated *"What is this limit, this limit may vary from person to person, some people want to be controlled by technology and external companies, maybe. And some people wish for this control themselves"*. On a personal level he had an clear idea what he wanted for himself. *"I have worked with computers in 30 years, so I do not fully trust computers. Therefore if I should have a smart home, I want it to be limited, not that everything happens on its own"*. He also, in general, focused on if the users should see a value in smart house technology, then it is essential to have a goal with it. But he also explained that often people do not have a purpose for investing in smart home devices and mentioned that this might be

Table 4.2: Statements related to control

Participant	**Statement**
P1	So, if your question was whether people **feel controlled** or that you lose autonomy that people follow what you do and collect data. So. So I do not know if you know the concept of the chilling effect? (...) The concept there is that if you feel that you are seen over the shoulder, or that you are unsure, or that you think your information will be collected, but you are unsure of what it is used for. Then it can lead to you refraining from doing something, or changing behavior. Because you think you're peeked over your shoulder.
G1	(...) that others **can take control** of it, that it is a scary thought, and can be perceived as yes a threat.
A2	I just know it at the surface that there is a need for autonomy, because it's for example it's my data so **I want to be able to have a say** on what can be done with the data.
A3	Yes, that's uh that's important, if you mean that the the user should have a **control of the whole system**, about what's being, like what data collected, and how the system would be controlled, and how the whole smart home would react.
I4	And then it may be the case that the solution should help **to give the customer control** then on, for example, their smart home, that it should be predictable and understandable what is happening, that they do not suddenly just turn on the light or it happens things that the customer has no control over. So it will be important part of understanding the needs, and whether the solutions meet the needs.

because it is more like a trend. **A3** also mention that there are individual preferences among consumers: *"I also believe that every user has a different requirement and* *preference on the system so it's important that these things are personalized."*

I2 and **I3** had both individual statements that stood out from the rest of the participants. When **I2** was asked about autonomy he immediately connected it to the importance of maintaining the position as a safe and credible company that the customers can trust. When he then was asked whether he believed that autonomy then was an important factor for maintaining this, he explained: *"Yes, I think more that the service is made in a way that allows the customer to be confident that nothing is being abused and that is probably autonomy."* **I3** talked about autonomy around that the users decision should be respected: *"Yes, to the extent that we always, that the user's decision, has in a way, shall say, is what decides. So let's say you have smart light in the living room then, the smartness says that you can turn off the light, but you turn it on, then we will in a way respect that, the decision that the user has made. (...) So that's how we will always, so that the system will always in a way try to ensure that what it thinks is right is right."*.

To summarise, among the participants there is some individual perception of autonomy in a smart home context. Since this is based on their first thoughts around autonomy in an smart home context, it is important to be aware that this can be affected by how autonomy was presented, and what the conversation topic was beforehand. However, many of the same topics were repeated by the participants, also between the different angles. These where: Data collection, relevant information given to the users, a trust relation between the company and the users, as well as transparency. However, generally the industry had a perception that the company and the system should help the user to get control over the system, where the three other stakeholders focused on that the user should be in control of the system.

4.2 RQ1: Is agency on the agenda?

As nobody mentioned autonomy directly in the first part of the interview, it was necessary to introduce the concept. However when this was discussed, almost everybody fined it important and mentioned that it to a certain extent was on their agenda. Even though most of the participants agreed that autonomy is a topic of importance, it varies on how they have it on their agenda and what needs to be done to ensure personal autonomy for smart home consumers. Because on thing was clear, it was not black and white so we need to get the grey areas out on the surface.

The industry, government and policy participants statements illustrate if they have this on the agenda in their company/organisation or not. **A3** which have knowledge of how industry work related to IoT was also asked if he believed if the industry in general have this on the agenda. The academics answered based on whether they see it on the agenda for researchers or if they have seen it in literature.

Figure 4.3 illustrates to which degree they themselves reflected on whether they have autonomy on the agenda. Here it is important to have in mind that this is based on their perception of autonomy and as we saw in the previous section it was individual how they interprets the term. The figure is based on the answer when they was asked: *Do you have autonomy on the agenda today?*

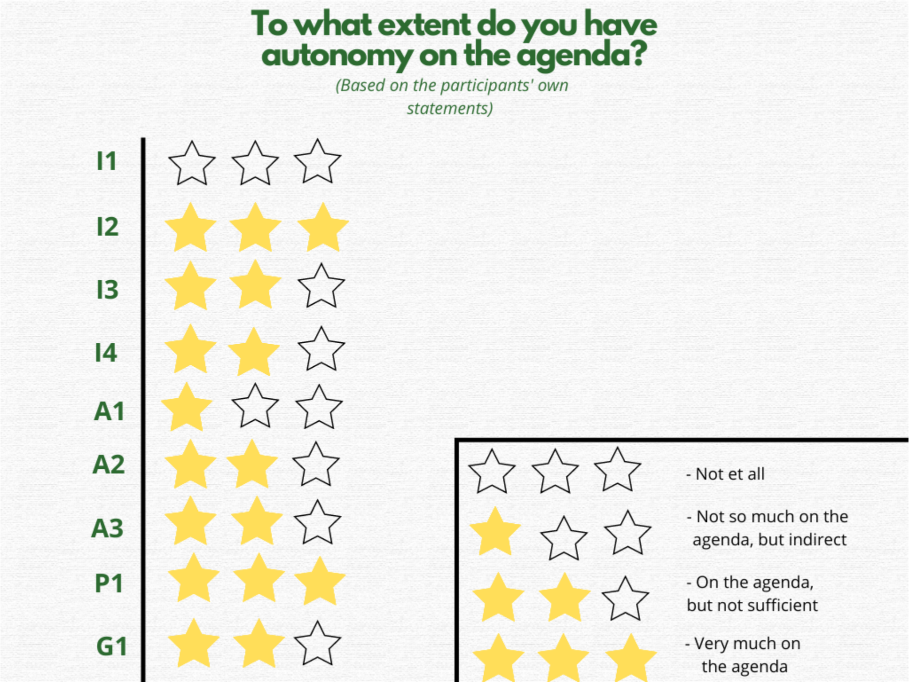

Figure 4.3: This graph illustrate to which extent the participant themselves reflect upon if they have autonomy on their agenda

I1 explained that it was not something they had on their agenda, he rather thought it is more about informing the customer and are confident that people growing up today has a common sense to technology. When **I2** was asked if he believed the they have autonomy on the agenda, he answered: *"Absolutely, that is [company name] highest degree of focus to maintain the position as a credible and safe and and a company that customers trust, so in a way, it permeates everything we do."* And was therefore categorised as he believed that they have it very much on their agenda. **I3** on the other hand explained that they have it on the agenda in the way that they will always design the system to try predict what the user want. He therefore focused on that it is important that the users intention is met and prioritised in the system. He also explained that it is important for them that their system does not change the way people live, and that the smart system should do things better and work in the background without messing with how people live their lives.

I4 also explained that they have autonomy on the agenda to the extent that they focus on that the product should be easy to use - so that the costumer feel like they master it. Also that the system should be predictable and understandable, so that the system contributes to giving the user control over the smart house. When asked directly whether autonomy is something they focus on in the sense of the word he answered: *"No, I do not want to say that that concept is somehow top of mind, I do not want to say, but it will in a way be implicit in some of the services that we have and that we develop. But that is in a way what we are looking for primarily, so it is not identified as in a way a key need. But it may be that there is something there"*.

A3 that has some knowledge of how the industry works on development of IoT was asked whether autonomy is something the industry talked about when developing solution, and for this he replied: *"I I think so, uh from there with the companies and the researchers that we have talked to, they always consider this as a priority, at least as a selling point. How to, to what extent that they can achieve this is still a question, this also need the more advanced technology, but I believe every everyone has this in mind, whether they can achieve this and when they can achieve this is still a question."* When asked if he think they succeed in doing it enough today, he answered:

"No it's not, it's not something that uh I can even see that happens in a few years in the future."

So it is clear that some of the message behind autonomy is of importance for the industry to maintain in the solutions (i.e., users wishes should be prioritised, enough information and extended control of their home), but the term has not been used as a key term among the three companies participating.

When it comes to the participant working in the governmental sector, he explained that they also have an indirect focus on autonomy, but also here, the word is not top of mined. However, it is relevant to emphasize that he also explained that smart home development was not relevant for them, because *"it is simply because we as a directorate should focus on the public sector and theirs - I should say need, and not into the private sector and we should not be in competition either with private actors. So therefore we do not think it is particularly relevant no."* Moreover, he mentioned that in the future it can be relevant for them to contribute with functionality for the public sector and mention health care as an example. *(...) "most obvious as our topics here it is after all, I shall say, authentication and authorization, so or identification then, up against what, shall I say, devices in the home or perhaps even more relevant on the body that gives - yes gives data about you as a person then, so* *there have been used examples with a blood pressure monitor for example, in health care, home nursing so that kind of thing, right, then it is so technologically possible to have a yes a form of monitoring then, and how that can be ensured in relation to identifying, what should I say, the user or the patient then, about whether it is safe enough and so on."*

The academics where asked if they or their research environment had autonomy on the agenda. When **A1** was asked if he had seen a focus on autonomy in research, he explained: *"In research, not directly, but in research we have in a way used in medicine that there is a very long process to approve some things when it comes to monitoring or smart sensor in medicine."* He also empathised that *"In smart home ok, I think in the future it may be that communication for example with older people or with fat people can come through smart houses, it is not, it is a bit pointless to have a new solution just for them, but it is not in a way prepared for it."*

A2 on the other hand has seen a focus on autonomy recently and that some project on the topic is starting to get funding. She has also noticed that this is something EU has on their agenda. *"So I think in Europe there is a lot of noise, not noise I mean uhm data sovereignty is the word. So there is a lot of efforts being put there so that the data about European citizens stays within yeah the boundaries and and then they are working on databanks, data stores so that your data stays and let's say, let's say your money stays in the bank and whenever you need to do for transaction you send it here or receive it, so the same way in databank you will have your personal information and whoever wants to provide you service or products, they talk to the databank and then the bank talks to you, do you agree to send this data, or if you get let's say 5 euros if you give your fingerprint for this purpose, and so I think the then the user have more autonomy than they can decide for what their data will be used and collected for"*. In other words, she explained that EU are working on solutions that can contribute give control over user data back to the users themselves. She also explained that it seems like autonomy is only in the starting phase: *"I think a lot of, things just started now, but nothing concrete, I see that people can really use it you know, the end users can make good use of it, because the market doesn't incentives autonomy."* **P1** explained that autonomy is highly on their agenda. And stated that autonomy *"is very very relevant to what we worked on"*.

4.2.1 Is the essence behind autonomy covered in standardisation and user tests?

It was investigated in the interviews with the participants from the industry as well as **A3** if it was any standardisation around maintaining control for the consumers, as well as if this was something they focused om in user testing. This section will first present the findings related to standardisation and then if the user test contains a focus of maintaining control.

Is there enough standardisation today?

The participants was first asked if there were established standards in IoT development. Their answers on this can be found in 4.3. It was clear that there is some standardisation on the low level, like radio protocols (i.e., Zigbee, Z-wave). Also on the hardware side there is a lot of standardisation on how smoke alarms and door locks should be designed. However on the software side, there is an agreement between the participants that there is a lack of it, and that this is because IoT is quite new. Nevertheless some new standardisation activities have started, aiming to make interaction between devices from different companies possible and easier, namely "Matter" that **I4** introduced.

Even though there is not much standardisation on the software side, it is not actually something the participants miss. When asked if they wished for more standards **I1** and **I3** agreed that this was not something the industry missed right now. **A3** elaborated that there are already good standards for the critical things, and that new well established standards will come on its own accord when more people start working on this. They all agreed that it is better to let the industry figure it out themselves as time goes by, also that the industry mainly want to regulate themselves. **I3** clearly mentioned that help from EU on this matter would not be helpful. *"If somehow the EU should try to do, GDPR is a nightmare. It is an example of how they create a system, and if it had in a way tried on some other things then it would have been just as problematic"*. **I4** on the other hand had another perception on this, and explained that there are some shortcomings on standardisation on the software part today, but that the new standard Matter would help solve the challenges associated with things not playing together and that it will be easier to make things be seamlessly for customers.

A2 on the other hand explained that she did not believe that IoT is enough regulated today in order to protect human users. When asked if GDPR, which is mainly the only regulation aiming to protect users in IoT today - is good enough. She explained that there are still loopholes. When asked what she is missing from GDPR she explained: *"GDPR doesn't govern the machine to machine communication and it doesn't talk about metadata in great detail so where the companies are exploiting, yeah the data"*. And explained metadata in the following way: *"Because it's not just you know, let's say I take a picture of a few, so it's not that just the picture is the private thing, the metadata about it is also private you know, where the picture was taken, at what time it was taken and looking at the pattern of you know, me taking picture of yours you know, at what time of the year and all those things."* **A1** had concerns that toady's standardisation not necessary are safe enough: *"And another*

Table 4.3: Is there many standardisation when it comes to development of IoT like on the software side?

Participant	**Statement**
I1	But there is very little standardisation on IT, since how should data, and that maybe what's a little surprising really, there is so little regulated on within IT and IT is quite new in that sense and IoT is quite new so.
I3	(...)But outer [layer/software] somehow when it comes to management app type stuff, then there is nothing, there is in a way no standardisation.
A3	There are um I wouldn't say a standard, but there are um kind of um so in different levels there there are standard protocols for communication for example, and there are also standard APIs, but I think more are still needed on for example the development methods and tools these are not so mature yet.
I4	Now between these major global actors, that is, they have set a common standard now that I do not remember the name of on the go" [Matter] (...) There is a type of industry collaboration now that standardises these solutions that allow the customer to buy in principle any type of gadget from any supplier, and it should be possible to connect to the solution that the customer has.

thing that I think is very important is safety, security - not always all these solutions, in my opinion, are safe enough." ***I: No it's not safe enough?*** *A3: "Yes that is my opinion. It is often based on standard solution which, may be, but is not necessarily good enough protected."*. So when it comes to standardisation and regulation, there are some disagreements between the industry and the academics.

When it comes to standard about securing the devices and the data that are transferred. They explained that then the same standards and best practices that are established for other software and applications are used. **I3**: *"There it is no difference between IoT and software in general somehow, we are talking about and*

Table 4.4: Do you miss any standardisation around this or do you think it is enough?

Participant	Statement
I1	Not often wanted to have a more complex and expensive system, it could be that it would have been better for the industry in the long run. I do not think enough..., I do not necessarily think we want it. The industry will mainly most want to regulate itself and not be regulated by others.
I3	We do not miss any standardization around it, it would have been a nightmare. If somehow the EU should try to do, ie GDPR is a nightmare. It is an example of how they create a system, and if it had in a way tried on some other things then it would have been just as problematic. So there it is much better that the software world, in a way, builds its own solutions there to be safe.
I4	Yes, it is so far, so it will be the initiative that refers to here [Matter] as which may help to solve the challenges associated with things not playing together and that it will be easier to make things be seamlessly for customers.
A3	I think it's uh OK at the moment, and the new standards will emerge as more people start working on this. I don't think standards is a bottleneck currently, for the most critical part there are already good standards. (...) We should let people try different things and the good knowledge can go into standard later, so from this point we don't think we are missing critical standards even though it's always good to create new standards as time goes on.

in a way make sure that you only in a way use best practices around passwords and two-factor and and such around data encryption and data encryption in transport". **I3** also explained that it is crucial for the companies to develop safe devices because if the customer's safety and privacy is challenged it might end up with huge economical consequences for the company. *"It is perhaps even more important to them that it is safe, than that it is for it is for you that it is safe somehow. Because if someone sees* *your living room then in practice it's probably not very dangerous really on the whole, but if if if Google's cameras suddenly stream out your living room then it's a huge commercial problem that will cost them billions of dollars as well"*

Then one can ask whether, since there is a lack of standardisation around the software part, can this affect the protection of the users? **A3** was asked if he thought the majority of today's smart home devices succeed in protecting human users. On that he answered: *"Probably not in that stage yet. I think more now the devices are more um, how the suppliers or producers of the devices are more on the features, so how to connect the, how to equip the physical world. (...) so the devices, is well yes also good to have a proper mechanism for protection in the devices, but the currently um it's probably, at least personally I don't see that this is a the top priority for the device makers."* When asked about what he thought they priority now was, he explained: *"The priority is still to a to get the proper functions working like if the if there's a sensor then the main thing is how to make sure the sensor can be used properly to capture the data they need, and also how this can be produced in cost effective ways so it can be scaled scale the soon."*

How does user testing works?

To investigate what they focused on related to user testing and whether this includes maintaining or ensuring autonomy for the users, the interviewees were first asked in general how these test works. They all explained that they tested prototypes on the users along the way and asked for feedback and changed the system based on this feedback. When asked what was important for them to look for in the user tests, it difference a bit between the participants. **I4** stated *"No, it's usability primarily then, in a user test where how customers experience the usability of products. If it is easy to use, there are some challenges, and as far as this is perceived to be useful and covers a need then."* It is also important for **I3** that the users understands the system, but also that there is a need to be a little cryptic: *"It is also to be I think also for us it is also a bit about being cryptic, ie out.. that is.., or having user tests where we, we see how the customer uses the product. Not so much to ask customers questions about what they want. (...) Because if you ask the customers what they want, they tend to, firstly, they tend to have a little bit of free imagination, secondly, it's like they are a little bit, it's a little bit like that. selecting right, so the people who have the strongest opinions about things they are the people who, do not necessarily represent most people. So it's a bit like customer surveys, feedback questions will often be very very nerdy, while because most people are like: it works, then it's fine by me"*

When **I3** was asked whether they had focus on if user feels that they have control even if things go on automation (i.e., if they test autonomy) he answered: *"No not,* *no we do not. Also because it is very difficult to test, so the way it is actually tested is the feedback that, because you will always get feedback if you feel that this is strange, but so so so for you somehow you can not really you can not test in any structured way that how it is experienced that the heat control turns on or does not turn on at 02.00 at night when you sit and watch TV somehow. It is difficult to make a structured test for it, so it's more just like that, you really just have to see that the customers give feedback and see what the customers do in the different situations, and look at the data more than feedback then."*. But he had also not experienced from his 10 years in this field that the user gave feedback of loosing control. **I4** answered that they focus on that the solution should be predictable and understandable, so that for example the light does not turn on or something else happens that the user do not have control over. **A3** was also asked if he thought autonomy was tested and based on his knowledge he also believed it would be difficult for the industry right now. *"uh that I don't know, uh no um no sufficient knowledge on this. But just by guessing I think uh based on what I know from the developers I think this is still a bit difficult for them at the moment, testing is already expensive on the IoT systems and testing with the human users involved is much more difficult, so I don't think its in there so, we're in the stage of doing this easily."* **I1** was also asked if he thought that user testing was downgraded if the budget is low, for that he answered: *"It is only natural that you are... the less competence or the less resources you have the more you have to sharpen it, but like that yes."*

4.3 RQ2: Use cases that needs more focus

This section present the findings related to which use cases within a smart home the participants mentioned that there can be concerns to. However some of the consequences where mentioned generally and not within a specific use case. They where asked general questions like: "If we take a look on smart homes in general, do you see some consequences / risks for people and society?", they where also asked to come with examples. The four most mentioned consequences are illustrated in figure 4.4. It difference in which use case they see these consequences, but some of them are illustrated in icons beside its consequence.

4.3.1 Manipulation and profiling

As mentioned in the previous sections, data collection was frequently mentioned. Further some of the participants stated that it can be consequences related to profiling and manipulation when the users data is used in a wrong way. **P1** explained: *(...) "If privacy is not built into those solutions and taken care of in a good way, then it will be quite a potentially intrusive amount of data. And if you also see it in the context of artificial intelligence and greater capacity to process things, so both hardware and software. Then such data points that a few years ago were just such useless data.*

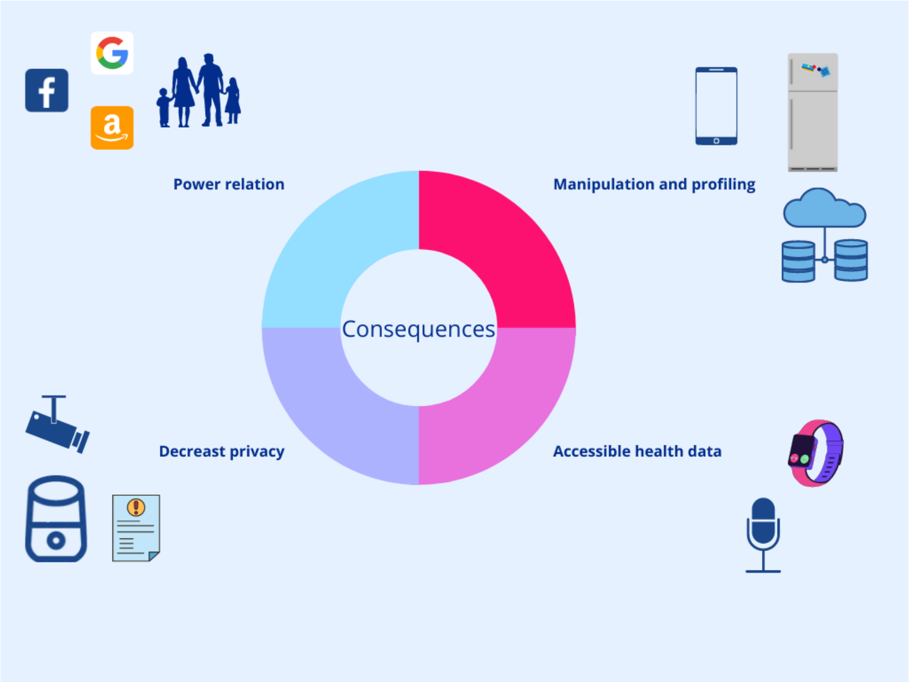

Figure 4.4: This figure illustrates the main consequences the expert mention related to smart home. Also in which use case within a smart home they where mentioned (i.e., smart refrigerator, smart assistant, smart watch, alarm systems). *The illustration is made with the tool and website canva.com*

Now it is possible to put them into a system and create a fairly detailed profiles of people." **G1** also had some thoughts about profiling and put it in the context of manipulation: *"If you compare with various social media about how fast they create profiles of you, whether it is Facebook or Spotify or others, that characterise you based on your usage pattern. Then I want - can say - a smart a smart thing with every conceivable details could quickly yes, make profiles of you that affect you so that you [for example] come to the store - so it sounds tempting if someone can remind you that it is empty in the fridge for milk, but then it starts to go a little far into the privacy difficult then, I think."*

Smart refrigerator in relation to everyday chores as food shopping in grocery stores was an example used by some of the participants. From the example above **G1** exemplified that getting a notification that you are out of milk when you are at the store can be a tempting thought, but at the same time that it might feel like it challenges the private life. **A1** also used refrigerator as one of the examples for illustrating the challenges with external companies' access to consumer data:

"General problem it is a big problem, because those companies can know all our habits, they have no information about people, but they have information about our habits: How much electricity do we use, if we invite guests - sometimes what we buy, what have we in the refrigerator, if connected. So this information of course is important and is in a way sensitive, but it is not information that is directly about people, but about habits". He also set data about our habits in context to manipulation, and emphasised that it is not the technology itself that have the possibility to manipulate users: *"It is not that technology can control us, it can be external companies that can control us, we must not forget that it is not smart houses that will do the job, but it is Amazon or Google that is behind it. And they have algorithms, they have, if it's just the algorithm of Google without people - it may be OK, but often there may be some human influence - maybe to sell the items we like or maybe not show anything from maybe competition - that we may be interested in."*

As mentioned earlier **P1** introduced the chilling effect and that it can result in change in behaviour. Also **A2** mentioned that manipulation and loss of choices over data being sent to third parties can make people do things they initially would not do: *"As I said you know about the seasonal interference it can interfere in people's decision making and we have already seen that you know, when we browse the Internet, how we are made into buying stuff that we don't want to buy, so just think of Internet of Things where you don't even have those choices. It collects a lot of data about you that you're not even aware of and then it is shared for these Internet companies and then we are bombarded with advertisements made into doing stuff that we don't want to go ahead with."* **A2** also focused on that this manipulation can happen to almost everybody and mentioned that manipulation within technology is nothing new: *"Yeah so people, if you don't have a very strong mind, if the people doesn't have a very strong mind and they will be subjected to manipulations, which we also feel normal people average people with average mental skills - I don't know what's the right word there, but you know, not the privacy scientists not the activist so the average population would fall into this trap of buying what the companies want them to buy and voting for what companies want them to vote for. And we have seen it in Brexit and in US elections through Cambridge analytical."*

4.3.2 Power relation

Power relation as a consequence of more advanced smart homes was also a recurring concern. Some stated that it can be multiple issues by giving to much information and thereby power to the big tech companies, where Google, Facebook and Amazon were mentioned as examples. Some of the participants also focused on that it can lead to power relation within a family or a household. In this subsection, the statements according to these concerns are presented.

I1 introduced power relation in a household in the following way: *"It is the other dimension that is actually a bit interesting, is this with, call it power relationship: you get one, maybe you have a partner in the house who is interested in smart house, and like that, and use this to keep track of the family, so it can be that the family does not know what data is there."* He also talked about an occurrence that he had seen in practice: *"Where a customer has bought a house and then they have argued about payment and then he has not transferred access to the smart house. Then he used it to turn on the light in the middle of the night to wake them up and almost terrorise them"*

I2 had also seen the consequence of power relations within a smart home also several examples within his group of friends: *"It's not, it's not, there are not a few smart houses either where it ends up that the man in the house is the prime mover to set it up and suddenly the wife and kids in the house can no longer turn on lights and such for it gets too complicated."* **I4** had a personal example on this matter: *"And for example here at home, here I have set up a smart home solution at home, and my wife is not quite online when it comes to how this works and so on, so she may feel a little like that a little powerless sometimes , somehow have to enter the app to turn on the light and it is not, instead of turning on a switch right, and that's the kind of thing can be experienced to be a bit frustrating"*

Some of the participants had concerns around that the increase in data collected by the big tech companies can give them a sort of power, and also enough information to preform a sort of manipulation as illustrated in 4.3.1. **A1** put it this way: *"Yes it can be dangerous, we give our in a way private information not directly about me or us, but some indirectly to companies, companies can not do this job, often without having this information so the ones they need absolutely necessary that they must have it, but in a way when they have it they can do anything with it."* **A1** also had concerns if we give external companies to much rights: *"But we must not give too much rights to smart houses. Again it sounds a little strange when I say that control to smart houses, it does not mean that it can be controlled by smart houses that are here, but it does mean that it can be controlled by external companies that look after smart houses, and it is the dangerous"* **A2** as mentioned earlier exemplified with Brexit and in US elections through Cambridge analytical which power the big tech companies actually have. On the other hand all the participants where familiar with that data collection of personal data is protected in GDPR. However, some of them mentioned that it differs from the companies how good they are to follow it, **P1** explained: *"And some companies meet the requirements [GDPR] in a very nice way, while others do not."* And **A2** put it this way *"So it's only I think the big tech which are trying to to award these fines and do the right things, but there are still many loopholes in the regulations that let them get away."*

4.3.3 Decreased privacy

In the report [Dat20] the Norwegian Data Protection Authority have in an survey from 2019/2020 seen a decrease in concerns in personal privacy compared to previous years. In several of the collected interviews, participants mentioned that the meaning of personal privacy has changed. **A2** explained it in the following way: *"For example if you talk about smart home, you know that traditionally, homes are the most private places that people used to have and when you bring in these IoT devices, wearable devices, smart lights, smart door locks, smart TVs, baby monitors, voice assistants, they are all ears and eyes for the companies from where they come from you know, so the home the privacy in home, that meaning has changed drastically."* She further explained that some of the concerns around these devices sort of vanish because they are normalised: *"Kids who are born these days, last ten years so they grow up watching these iPads, iPhones and all kinds of phones around, and sharing information is very much fine, it's very normal, you know, so."*

I3 explained that his experience is that people are just concern if they do not see the value of the product: *"Now it is the case that people, my experience is maybe a bit there that people are only worried about safety most people then are only worried about safety and trust and all this, as long as the product does not, as long as they do not understand or they see the value of the product and after they see the value of the product then these things are suddenly really a bit irrelevant to them."* He exemplified it with the use of microphones in the house, like Amazone Alexa and Google Home: *(...)"Also like Amazon Alexa, Google Home all these right, people are like that it's very scary with a microphone in your home, but you bring a camera and microphone to the bathroom somehow. You sit and sit with your cell phone on the toilet and and and there are cameras in all directions somehow and you are not worried about it at all."*

P1 illustrated that voice assistant can have consequences: *"For example, you can imagine that a digital assistant then, as you can tell what to do and that means that it must always really listen. If you do not trust it if you do not trust that the information is deleted or not passed on. Do you then dare to have confidential conversations with your partner in the home, so there are some things you do not want to talk about in your own home maybe the political thing, maybe it is about you being part of a minority maybe, yes there is one example then that it may have consequences."*

I3 also introduced a very unfortunate incident that has recently been seen in the media: *"As you have probably seen now with verisure right, where verisure Sweden has suddenly had problems with the fact that they have made decisions that their cameras, that cameras are visible, ie camera images are visible to the alarm center, where employees and and and and people and the alarm center staff have then shared* *pictures that they have seen when they have seen people who have triggered their alarm naked or something, and then they have in a way shared this internally at the alarm center then, like go and look at right, customer 34 2 74 because there are nude pictures right."*

4.3.4 Accessible health data

Although many forms of data collection was mentioned by the participants, health data stood out a bit. This because it was mentioned that devices that amid to use health data are more regulated then devices that do not aim to collect health data. At the same time, concerns were raised with respect to smart home devices that are not initially intended to collect health data, but that might indirectly have access to it anyway. For example through voice assistant that has been mentioned earlier.

P1 explained that the use of health data is heavily regulated: *"If it is a product that is used in health, then there is separate legislation there ehh that goes on product safety and other types of things then. Quite a lot of regulations a bit depending on what it is to be used for in health"* **A1** explained that it possibly could be connection between smart houses and some health data: *"But there are many things that are, can be critical for example if there can be link and there can possibly be link between smart house and some health data, so there is completely different way way to assess, you are not allowed to send medical data on regular network, you must have special requirements"* He also explained that he have contributed in projected where they have tried to fulfil these requirements: *"It is very difficult, in many of the projects we were unable to implement all these requirements - to have such good protection."*

G1 explained that there is a fine line between what the data can be used to before it maybe becomes a challenge: *"That Spotify preaches and find out what kind of music you like I think is quite harmless, but if it comes to health information and yes one says that they can say something about mental health, then it becomes even more difficult and scary I think."* He also exemplified with the use of smartwatches: *"No this is a very, should say challenging field [health]. As we mentioned earlier, it is you as the user who must have control, and if you take a comparison then or something that is already there, then these are smartwatches that are really health information, and which I experience that many people uncritically use and set up, and it says if you then combine it then, heart rate is quite normal right, but if you then combine it with blood pressure for example then you may have some new indicators then.*

4.3.5 Use cases

Some use cases (i.e., smart home devices) were mentioned as examples for illustrating the consequences above. Namely: Voice assistant, smart refrigerator, alarm systems and smart watches. However, the concerns was not necessary to one use case itself, but more about smart homes as a whole. That the increase in data from different devices can lead an incredible amount of different data, and with the technology that exist today, these data can be set into a system and make quite accurate profiles of the users, as **P1** mentioned earlier. The huge amount of data and the profiling can then lead to consequences, including the once mentioned above.

4.4 Suggested solutions

4.4.1 The right information to the users

Generally there was one thing that was repeated in the interviews, the importance of that the users get the right information and more educational awareness. Either by making people became more privacy aware, general knowledge about Information and communications technology (ICT) and that they should know what they want from the devices before investing in it. **A1** raised concerns with that the knowledge about ICT is to low in the population: *"But maybe it can also be another reason that people do not have enough knowledge in ICT. ICT in general, I think there is very weak knowledge in ICT - it must be greater in the environment and in society"* What the consumers need more information about was as **P1** stated *"And I also believe in understanding data flow, how it is used, how it can be misused, what is the risk"*. The participants agreed that it is both the company that produces devices and the governments responsibility that the people get enough information and awareness around technology. But also that the users has the responsibility of acquiring the knowledge they need.

There were in general also two concrete suggestion on how to improve the information flow to the consumers. The first is availability and more advanced methods to ensure that the information reach the customer when they need it, **P1:** *"There I think that there are many who have a lot to go on as it is about providing information when the person needs it, ie you can have a privacy statement that is there and is available both before you buy or use a product, while you use it and after you have finished using it so that that information will always be available (...) But that there may also be such type of pop ups or other ways of communicating with the user to help users understand that their information is being used and and how. So there is definitely a lot of potential to get even better"*

The other suggestion is that it should be a part of the curriculum in school: **A2:** *"I think we should just like we teach in kindergarten what is moral, ethical behaviour - so you know - there should be some requirement from yeah if I can call the state - the Norwegian state. It, you know, it must put some basic introductory courses in primary school, high school, and universities where people are told about what is privacy, and and what needs to be taken care of and, what should be our choices and,* *the risks associated with those choices and yeah it should come in the mainstream."* For as **A2** clearly stated, this knowledge is not covered today:

A2: "I have a PhD, I have two masters and schooling etc., I never went/came across a course that teaches you, that is mandatory for you, "that this is how you read a privacy notice and these are the consequences if you consent to or not consent to"

4.4.2 Certifications

A consequence of a relatively new marked with many new innovation, but little standardisation is that it might be difficult for the consumer to know which product are safe to use and meet their needs. **I4:** *"Yes, so it's a bit like that, today's fragmented market can be a bit confusing for customers I think. And not all solutions work together so the safest thing for the customer is to buy a solution that meets the needs they have then, from one supplier. This is perhaps the safest thing to do, because then in a way the supplier has put it together".* As a solution for making a better overview for the consumers some of the participants mention that a certification scheme might be a solution. This is not covered to a great extent today: **P1**: *"There is also an opening for certification schemes and industry standards in the regulations. There have not yet been so many certification schemes for this here in Europe nor in Norway."*

When **I1** and **I4** was asked whether they thing certification schemes can contribute to more trust for the devices they answered. **I1:** *"Absolutely, there are some already if you have a product with support on ZigBee or Z-wave then you know that OK it is certified it creates trust so it is the industry standards that are established".* **I4:** *"yes yes then, that there is a possible way. (...) So it must, then you must have a very good certification scheme and have one, have some actors then who take on the role of certifying. So it's a bit like that kind of half complex and it should probably be a yes preferably such a type of global certification for you to be able to get a volume on this, you can imagine a national certification or in the EU type as an alternative, or the third alternative is to let us say that a company, if we had a service, we could in a way have a certification scheme for equipment that we have tested and that we know works with our solution so it could also be a way to go then. Then I do not have a clear idea of what the best alternative is, the best thing would be if you got it globally, but I do not know what it takes to make it happen."*

4.4.3 Protection by design

A2 and **A3** had a focus on that user control should be included in the design process from the very start. **A2** explained *"right now they need to develop privacy by design and it's going to take its own time."* **A3** explained that the users should be put in the centre from the very beginning. *"I think from the very beginning and let's say that application development from the beginning you should put the user in the central of the whole design process to consider what they actually need and what might goes wrong, might go wrong a when the system will be used, so all these should be considered in the very beginning when people start designing things."* **A2** also explained that there are companies that try to give more control to the users in their design today, and exemplified it with how Apple gives information to their users. *"For example Apple, there's a lot of endorsement on showing how they're taking care of privacy, that our data stays within our phone."* So in general they explained that one solution to the problem can be to include the users need, including autonomy in the design from the very beginning.

4.4.4 Local data processing

A2 suggested that if it was possible to remove the need for transmitting data outside the home, it would help establishing trust for the consumers. *"So if we can develop technologies that doesn't require it to be sent outside the home, the home data, you know, if it stays within the home, so then we can trust it more"*. **I3** was asked whether it in theory is possible to process the data locally: *"No, it would not really have been possible, so you could imagine a system where your mobile phone sent data to the gateway in your home and the gateway in your home ran all this here locally. The problem with that is that, firstly, it would make the gateway much more expensive because you have to have a much stronger computer, the second is that you do not have the opportunity to learn across, so you can not do more such aggregated lessons about how fast how fast it usually takes to heat a house then. So so so it is clearly technically possible to do everything we do on the server locally, but but with that, it would quickly come up in so has gotten into, the other problem of smart house, which is the little there that, you do not know that you want smart houses before you have smart houses, and if it is very expensive to have smart houses then you will never get there."* As he explained it is technically possible, but there are some barriers that makes it complicated.

4.5 Summary of the findings

This section summarise the most important findings done through the interviews.

I found that there are different perceptions of autonomy, not just between the different stakeholders, but also within the stakeholder groups. In general, the industry participants focused on that system or the company should contribute to better control over the users smart home and that it is crucial to maintain a trusting relationship with the consumers. The rest of the participants however, focused on the importance that the users had control over the system or the data collected by the system. It was discovered that the term autonomy was not a key term in smart home development. However, almost every participant explained the importance of what is covered by the essence of autonomy (i.e., being in control of our self and our environment), but it varies to which degree they have it on the agenda today.

As far as discovered in this thesis, there currently does not exist a framework, standardisation nor testing schemes that aim to directly protect users autonomy in smart home development. Consequences of smart home use that were most frequently mentioned by the participants were: Profiling and manipulation, accessible health data, decrease in privacy and power relation. The participants also come with suggestions for solutions that could contribute to increased autonomy for the users. Namely, more information to the users and educational awareness, certification schemes for smart home product and protection by design which include considering user autonomy from the very start of designing and development of the devices. Also that if devices were developed with a solution where data transferring outside the home was removed, it would lead to more trust for the users. With the findings fresh in mind, it is time to discuss whether autonomy is on the agenda among the different stakeholders and what the consequences for consumers and society might be if autonomy is not ideally dealt with.

Chapter 5 Discussion

5.1 Is human autonomy misinterpreted by the industry?

The results from the interviews indicated that human autonomy was generally not a recognized term in the industry, with no standardization nor testing methods applied in practice to ensure that autonomy is maintained for the users. However the essence of autonomy is indirectly, to a certain extent covered. In this setting to get the users a form of control, but not necessary over the systems performance and own action in relation to the system, rather more control over your house (e.g., power consumption). One industry participant however, focused on that the system should prioritise the human users' self-determination and ability to act. Moreover, according to industry developers, the technical design would meet the human autonomy requirement if users were informed about the type of data collected and how the system worked to ensure that nothing could be abused. No mention was made concerning human users having direct control over the design process; thus, this might not be significant design considerations for the industry participants. Even so, one respondent among the industry participants mentioned that the system should be designed to help the user get control over the smart home solution itself. Overall, the system design should be as predictable and understandable as it can be for the human user to comprehend actions, but not to the extent that the human users can have a direct effect and decide the outcome. The academics, on the other hand, focused either on that the users should have control over the whole system or their data. Also, that autonomy in smart homes is dependent on what the users want for themselves, and it might be individual preferences on this matter. Therefore, the focus on personalization is relevant for ensuring autonomy for a diversity of customers.

This thesis argues that human agency/autonomy is maintained if users feel that they are in control of themselves and their environment, and the definition for human agency used throughout this thesis is: *"The ability of individuals to influence and control their own motivations, actions, and environment"* [KK20, p.4][Ban01]

One can argue that the industry perception of autonomy, partially, did not match up to this definition. Their understanding of protecting human autonomy can be seen as a paternalistic standpoint, as opposed to seriously addressing the increased responsibility of the technical design caused by the technology's pervasiveness. The existing protections were sufficient, as long as the human users' were confident that nothing could be abused by being informed about the purpose. It is possible to interpret the industry participant statements in light of that the company knows what is best for the users and, therefore that a trusting relationship between the company and the user is more of a marketing exercise. Another reason for applying this interpretation of the industry perspective is that one participant mentioned that it was important for them in user tests to look at how the customer used the system rather than ask them what they wanted the system to do. This may indicate that the company makes the decisions when it comes to what the user might want and need, which is also an indication that the company knows what is best, also in terms of what the users might want. The academics' perception, on the other hand, matches more up with the definition of autonomy provided by this thesis, as their focus was more on that the user should be in control over the whole system or at least the data the system collects.

However, it is not strange that the industry might look at this in a paternalistic way; as some of the participants indicate, the knowledge of ICT is not well established in the general population. Then that people with education in ICT and who work with it daily would better understand it is not an unfair statement. However, in the process, literature suggests that it will be a loss of personal autonomy if people do not know how the system works and are not given the opportunity to act based on what they personally want. The perception of autonomy as a technological construct also varied a lot among the participant and does not always match up to the definition on which this thesis is based. When that is said, there is also a broad specter of different definitions of human autonomy and agency in a technical context in literature. This illustrated the need for consensus around this concept before it is possible to initiate action on how to ensure that the user maintains control over their smart homes.

The European Commission has recently put forward a reference point on key rights and principles for digitization through the European Digital Rights and Principles. EU wants to ensure the population of Europe that they can appreciate the opportunities of technology and make sure that their right as humans is carefully considered with a human-centric approach [22]. This new declaration will most likely affect the industry in a way that they need to have human-centered design approaches higher on their agenda. This thesis argues that the maintenance of autonomy and the ability to initiate own actions fully are important factors for succeeding in this matter. Further, there is a need to develop a framework that can work as a standard in developing the IoT devices that ensure autonomy for the users.

5.2 How to achieve the right balance between human and device agency?

The preferred balance between human agency and device agency, seems to be an unsolved mystery. As [CMK+12] suggested that *"beyond a certain level of assistance by a device, users experience a detectable loss in their sense of agency."* [GC22, p.4][CMK+12]. The loss of agency can have negative consequences for the users, such as changing behaviour due to interacting with the technology and refraining from doing what they actually want. At the same time, the right balance (i.e., when human agency and device agency are shared in a preferred manner) can have a positive effect on human life [JWJ+12] [KK22]. As exemplified in Chapter 2 it can free the users' from unimportant decision making [GC22]. It can empower the owners of the device by using energy more efficiently, and today's increasing electricity prices can have a huge impact on the users' economy. Furthermore, in general, contribute to making life more interesting [SF20]. How to calculate this balance may depend on different factors, **A1** in the interview stated that individual preferences might play their part.

A1; *"What is this limit, this limit might vary from person to person, some people want to be controlled by technology and external companies, maybe. And some people wish to keep this control themselves"*

The fact that every human is different and has different desires may also affect to what extent they are willing to share the control with their smart house. A related challenge might be if the people that live in the same household have individual preferences on this matter. In the interviews, several examples were mentioned where one in the household installed the equipments, while the others where unfamiliar with how it worked and which data is collected. Different individuals decide to install a smart house, versus those who live in the house and experience being serviced by the system. For these users to have any control, they need enough knowledge and information to make an informed choice. **A1** also pointed out the importance that users see a value in the product before they buy it, otherwise, they will not necessarily experience a positive effect of owning and using the product. He also stated that he experienced that many buy smart products without knowing exactly why and mentioned that it might be because of strong market forces or trends.

G1; *"That Spotify predicts what kind of music you like, I think is quite harmless, but if it comes to health information and yes one says that they can say something about mental health, then it becomes even more difficult and scary I think."*

G1's statements illustrate that it, to a certain extent, is useful that technology can predict our desires. However, there is a fine line before it might be perceived as uncomfortable. Maybe it becomes a problem when people consider highly sensitive data is included, such as health information. If users had more hands-on control over which data the devices are allowed to use, it might help minimize the problem. From the literature presented in 2.1.1, increased control of personal data was a desire from human users and was also a topic mentioned a lot in the interviews. **A2** presented the EU's work on sovereign identity as a possible solution to more autonomy over personal data. That includes a type of data bank that the users control, and when actors want access to any of the users' data, they need to send a request to the data bank where the user provides consent to allow the access. In that way, the users have better control over which data they allow for usage.

A2 gave some praise to Apple's way of informing customers about how they deal with privacy: *"for example, Apple there is much endorsement on showing how they are taking care of privacy, that our data stays within our phone"*. She further empathized that if IoT devices could be designed in a way that data do not necessarily need to be transferred outside the home, it would be easier to build trust: *"So if we can develop technologies that don't require it to be sent outside the home, the home data, you know, if it stays within the home, so then we can trust it more"*. **I3** was asked if data in theory can stay within the home. He explained that there are some technical barriers before that can be a reality. Where one of the reasons is that especially AI technology 'learns' and optimizes from the data. Moreover, he explained that cost is a central factor here, but that it in theory can be possible.

Some years back, high cost, battery life, and transmission distance were technical barriers. Today, ZigBee and Z-wave have solved some of these challenges. Maybe in the future, it can be possible to develop gateways that can handle the process locally and at the same time be cheap enough for consumers to invest in it. Furthermore, as the transmission of data is core to the problems for why we might have a decrease in privacy, as well as the uncertainty of surveillance - it might solve some of today's challenges for ensuring trust and more control for smart home uses. However, as **I3** suggested, it might lead to new technical challenges.

There are many cases where smart home devices can be beneficial, such as those that help reduce power consumption and improve air quality. However there might be situations where smart devices should never interfere. For example, in combination with highly sensitive data like health data as mentioned above. The literature also suggests that tasks that include personal feelings, thoughts, and moral grounding should not be available for smart devices, as feelings, private spaces, and security are frequently stated as areas where the users would like to be in total control [SSA+19].

As observed from the interviews, the only direct control given to the human users of the IoT system is through GDPR. The GDPR is also the most important foundation for the industry to tackle the agency disbalance and protect human users. Even so, there are indications that this balance is not fully dealt with today. As GDPR mainly covers data protection and not measures to ensure user control over the whole system. European Digital Rights and Principles can work as guidance for what the main goal should be. However, there seems to be a lack of concrete technical measures for the industry to follow to reach this goal. So is there a need to change practices and technical solutions to protect the maintenance of human autonomy?

5.3 Is there a need for change in how autonomy is solved technically to ensure freedom for the human users?

From the result of this thesis one can argue that the focus on maintaining user autonomy in the system configurations is not covered robustly enough in the industry today. Maintaining increased user control in the system seems like an obstacle for the industry. Since there are indications that the main focus is to get technical features and functions to work correctly. However, it should be mentioned that **I3** explained that the feeling of being in control is hard to test in practice. It, therefore, seems like there is a lack of testing framework or framework in general that can contribute to enhanced control for the users. Even though as **A3** stated, he personally believes the focus today is to get the technical functions to work and that protecting the human users is not the top priority for device makers today. They also do not want to be regulated by anybody and wish to regulate themselves; where one of the reasons for this is that it will make it more difficult to get the technical features to function correctly. So there seems that protecting the users is a barrier to the technical development in the industry today. To user test properly is as **I1** stated in the interview downgraded if the budget is to tight, there are therefore indications to believe that today it is mainly the commercial and technical incentives and feasibility that determines the balance between human agency and device agency.

The academics, on the other hand, explained that there is not enough regulations for protecting human users today in IoT, and that there are still loopholes in the established regulation. One loopholes is as **A2** explained metadata. She exemplified it with picture taking. It is not just the picture that contains private information but also the metadata, for example, when, where, and by whom the picture was taken. This is according to **A2** not protected through GDPR at the moment.

One of the reasons why protecting user control in the system is a technical obstacle, is that it might not have been included in the design requirements and technical specifications from the start. **A3** suggested that the users should be put in the center from the beginning when developers start to design the devices. This includes what the users actually need, desire, and want to control and what might go wrong when the system is used. In the literature, it is also suggested that users should be allowed to exercise control in all phases of smart home deployment and use. That includes before purchase, during configuration, and through normal operations [ZGM+19].

Therefore, there are indications of disagreements among the industry and the academics on how to protect the human users in the smart home environment. As **I3** clearly stated that GDPR is perceived as a nightmare from an industry point of view might illustrate that there is room for improvement on how new regulations can be presented. It was evident in all of the industry interviews that they want to provide useful services to its customers and that a trusting relationship is crucial to maintain. **I3** pointed out that one small mistake from the company mostly fires back on the company economically. For the industry to have the opportunity to keep developing these devices, financial profits are vital. Since GDPR brought a massive transformation for business, it was also expensive and can therefore have consequence on the user testing budget. So, even though one can argue that GDPR was essential to receive more control for the users, it can have impacted the users negatively in other ways - for example, the ease of use of the system and the opportunity to come with feedback if the company had to downgrade user tests because of economic reasons. The results from the interview illustrates that even though there was some disagreements between the participants on how user protection should be done, they also agreed on one thing. The importance of maintaining trust. This agreement can be used as a starting point for agreeing on a obstacle - how to better ensure user control in the design process of the devices.

The following options could technically address the current limitations in addressing human autonomy and are based on the participant's suggestions for a solution.

- Plan and build user control from the beginning.
- Educate consumers on the responsibility of protecting their personal autonomy and include certification schemes for smart home devices. So that it becomes easier for the consumers to navigate the market.
- Ensure user control through laws and regulations.

In order to build a framework that ensures human control and autonomy, this thesis argues that it is for everyone's benefit that this is done in cooperation between different stakeholders, for example, the stakeholders focused on in this thesis. Since by including different perceptions and points of view, it might be easier to develop a framework that actually will work in practise, and where the main goal should be to protect the users.

5.4 What impact does the loss of autonomy have on individuals and society?

This thesis has highlighted four consequences that can emerge from smart home technology: Manipulation and profiling, accessible health data, decreased privacy, and power relation dis-balance. These consequences were frequently mentioned in most of the stakeholder interviews and illustrate that the smart home industry must carefully consider avoiding harmful outcomes when developing smart devices. But, what happens if these consequences are not dealt with?

Decreased privacy was a consequence mentioned by some of the participants, mostly by the academics, policy and government participants. In [Dat20] the results from several surveys show that a small proportion of participants in the age group 15-19 is less concerned with their privacy now compared to 2014. As **A2** mentioned in the interviews, sharing information about oneself is common today. And that the meaning of privacy has changed drastically. This might be one of the reasons privacy is less important for the youth in the survey, and that one's own desire to have privacy control might decrease as sharing becomes more and more common. However, the results from the survey [Dat20] show that privacy is still important for most people. At the same time, the privacy paradox seems to stand firm. **I3** mentioned that people are concerned with microphones in their home, but at the same time it is common to bring the phone to the toilet - a phone that in theory is both a microphone and a camera in both directions. If people feel that they sacrifice their privacy when using technology and lose control over it, this might lead to distrust against digitization [MPA19].

Another consequence of increased accessible data about users is profiling and manipulation. It becomes easier to make custom advertisements and make people do as the companies want. This may lead to users not doing what they actually want, and in the worst case losing their potential to determine their future. **A2** also mentioned that most of us would be easily susceptible to such manipulation. As an analogy this is comparable to always having a salesman in your own home, always trying to make you buy things you do not need. In other words, this is most likely not something that most people want.

Health data are one of the most protected data today, however, in the interviews, there were concerns that smart house technology indirectly can collect health data, for example, through voice assistants. If the capture of this type of data is a reality, it would be a significant intrusion into people's private lives. The Norwegian government has a significant trust among the Norwegian population [Dat20]. **G1** explained that in the future it can be possible for them to contribute with features for ensuring security in smart home systems, mainly for the public sector and especially in health situations. Further, **A1** explained that it would be pointless to develop a totally new system just for health situations. This indicates that it might be relevant for the public sector and the private sector to cooperate in order to build smart home systems that are safe enough for use in relation to health and sensitive health data.

Unbalanced power relations within households were also mentioned in several interviews. If one person in the house installs the smart house, it might lead to others in the household not knowing what data is collected, how the system works, and even being unable to use and access the system. A considerable consequence is if we start to limit ourselves by adjusting our behaviour, because we feel observed and avoid doing activities we believe can lead to negative consequences later. One example is to refrain from searching certain keywords online or avoid having sensitive conversations inside your home because of fear of surveillance. These effects challenge human rights and freedom of speech and can interfere with how people obtain the freedom to live their lives on their terms.

It seems like there is a "deal with the problems as they appear" attitude in technology. However, we do not know about all the psychological, cognitive, and behavioural consequences of gradually losing control over smart homes. This thesis argues that this approach should not be standard in technology today. Because we do not have many more chances with the consumers if they keep seeing that they lose control - this study does not believe that consumers will give so many new chances for the industry to do it right the next time. Rather the position of this paper is the importance of dealing with the possible consequences right away and implement protective solutions in the design. In a world that keep changing and moving forward, it is important for human to have something safe and something they can control. In many cases, this is humans private homes, and the technology should not take the control away from them.

Developing a framework that ensures human control in smart home development that also includes protecting autonomy might take some time. There are clear indications that the work on autonomy in a technical context is in an early stage, as **A2** explained in the interview. In the meantime, there should be a focus on educating the general population in ICT and how they can protect their privacy. As technology is starting to affect humans lives so closely it should exist no doubt about how important it is that people have enough information about it, and understand it. This thesis suggests that more knowledge about privacy and technology should be included in the curriculum. Because when **A2** that has two master's degrees and one P.h.D. has not learned how to protect her privacy through schooling, it is not covered enough today.

So how autonomous and free are human users? If we move through a time where we no longer choose the music we listen to, do not decide what we will eat or watch on TV, if we change behavior because we are uncertain if we are monitored and refrain from doing what we actually want. And if we gradually lose our potential to determine one's future, then there is ground for a new discussion on whether we go in the wrong direction of freedom. However, as discussed above this thesis argues that technical measures can contribute to giving more control back to the users, and implementing these correctly would ensure a successful balancing act for all parties involved.

Chapter 6 Conclusion

From a psychological point of view, autonomy and the feeling of being in control are crucially important for humans' health, wellbeing, and safety [Ski96], and it should therefore be protected in technology. However, there seem to be indications that the focus on protecting human autonomy in a technical context is only starting to be on the agenda in the technical development of smart homes in Norway. The perception of autonomy varies among multi-disciplinary actors, consumers, policy, industry, academia, and government, lacking any conclusive and common regulatory framework or ethical standard from scientific literature and expert point-of-views. Conflicting perceptions are reflected, for example, how industry participants prioritize and act toward integrating human autonomy in the technical development of IoT solutions for consumers' home. The findings indicate that protecting human agency and autonomy is an obstacle for the industry today, since smart home technology is a relatively new innovation and ensuring that the functionality works as expected seems challenging enough. In order to come closer to a more balanced solution on prioritizing human versus device agency, this thesis argues that an agreement on the meaning of the terminology can be the first step to ensure autonomy for human users.

The fact that no legal, regulatory, or ethical framework exists to standardize and structure user testing that maintains human users' autonomy illustrates the lack of the highest form of human protection in today's IoT solutions. Even so, the industry participants agreed when considering if the level of standardization was sufficient to protect human autonomy today. However, the academics disagreed on this and explained that there is a need for more regulation and better standardization to ensure autonomy, and make the systems safe enough. This thesis also found that the General Data Protection Regulation (GDPR) was today's most relevant regulation that focuses on protecting users. However, several participants' expressed that GDPR had some shortcomings and loopholes. One of them was that it does not include metadata protection, where no legal standards exist. With that said, there are clear signs that new regulations are rapidly forming; for instance, several new EU policies are implemented.

If human autonomy is not considered in the technical design, it can lead to unfortunate consequences. This thesis has identified issues such as consumer manipulation and profiling, decreased privacy, power relation and accessible health data, as the most frequently mentioned consequences by the participants in this thesis. With that said, how people will react to a loss of autonomy is, as far as this study has discovered, to a certain degree, unknown. One concern is that if people repeatedly feel a loss of control over technology, it can lead to increased distrust and feelings of ambiguity among human users' towards rapid technical innovation. Therefore, this thesis argues that further research on this topic is of great importance. This can be done by developing a shared design framework for use in the development process that ensures that human autonomy is maintained in interaction with smart home devices. The design framework can be developed in cooperation with multiple stakeholders operating in digital societies, for example, industry, policymakers, academics, and government, supported by multi-disciplinary experts that can bridge technical and social science. Moreover, this thesis argues that increased efforts in informing and educating the general population in information and communication technology are essential for a more diverse representation of voices in society. Then, the general public can make informed choices about protecting themselves and their privacy. After all, people should fully control their own home and lives.

6.1 Suggestion to future work

This thesis has found a lack of holistic and common consensus on the definition and meaning of human autonomy in a technical context among the multi-disciplinary stakeholders, both among expert opinions as well as in scientific literature. As a result, future research should address the development of a common understanding of the terminology crucial for building a design framework that can assure that autonomy for the users of smart home technology is protected technically. Therefore, addressing a shared terminology would be a logical starting point for further scientific development on this topic.

Furthermore, developing a shared design framework that can maintain autonomy for users in a smart home would benefit from contributions from multiple perspectives and stakeholders. The stakeholders included in this thesis (i.e., industry, academics, policy, and government) can be complemented by participants from social and health science research. The rationale is that human autonomy is a topic that is well understood in medicine and social science, and it can be of value to include this experience and their point of view. A suggestion for reaching consensus and developing a shared design framework is to apply the Delphi method as introduced in 3.2. The Delphi method is a well-established method for reaching consensus and combining multi-stakeholder opinions into a common result that can benefit several perspectives in society.

References

[19] *Official legal text*, Sep. 2019. [Online]. Available: https://gdpr-info.eu/.

[22] *European declaration on digital rights and principles for the next decade*, The European Parliament, Brussels, Belgium, 2022. [Online]. Available: https://ec.europa.eu/newsroom/dae/redirection/document/82703.

[A C12] J. J. A. Cavoukian, «Privacy by design in the age of big data», pp. 001–021, 2012.

[Ada20] A. Adamo, «Taming the Techno Leviathan: Why We Should Adopt a Society-in-the-Loop Model Inside IoT Utilities», in 2020.

[AF15] S. Applin and M. Fischer, «Cooperation between humans and robots: Applied agency in autonomous processes», Mar. 2015.

[All17] M. Allen, «Informant Interview», in *The SAGE Encyclopedia of Communication Research Methods*, 2455 Teller Road, Thousand Oaks California 91320: SAGE Publications, Inc, 2017.

[Ant22] F. B. Anthony Salvanto Jennifer De Pinto. «Cbs news poll analysis: After two years, most say covid divided the country». (2022), [Online]. Available: https://www.cbsnews.com/news/covid-divided-u-s-opinion-poll-analysis-2022-03-17/ (last visited: Jun. 9, 2022).

[Bah21] M. K. Bahus. «Selvbestemmelsesrett». (2021), [Online]. Available: https://snl.no/selvbestemmelsesrett (last visited: Apr. 26, 2022).

[Ban01] A. Bandura, «Social Cognitive Theory: An Agentic Perspective», *Annual Review of Psychology*, vol. 52, no. 1, pp. 1–26, Feb. 2001.

[Bio06] F. Biocca, «The Cyborg's Dilemma: Progressive Embodiment in Virtual Environments [1]», *Journal of Computer-Mediated Communication*, vol. 3, no. 2, pp. 0–0, Jun. 2006.

[Bun22] M. Bunz, *How Not to Be Governed Like That by Our Digital Technologies*, English, ser. New Critical Humanities. Rowman & Littlefield International, Feb. 2022.

[CB14] J. Y. C. Chen and M. J. Barnes, «Human–Agent Teaming for Multirobot Control: A Review of Human Factors Issues», *IEEE Transactions on Human-Machine Systems*, vol. 44, no. 1, pp. 13–29, Feb. 2014.

[CBGT18] J. C. Cano, V. Berrios, *et al.*, «Evolution of iot: An industry perspective», *IEEE Internet of Things Magazine*, vol. 1, no. 2, pp. 12–17, 2018.

[CG16] J. Colnago and H. Guardia, «How to inform privacy agents on preferred level of user control?», in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, New York, NY, USA: ACM, Sep. 2016, pp. 1542–1547.

[CMK+12] D. Coyle, J. Moore, *et al.*, «I did that! Measuring users' experience of agency in their own actions», in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, May 2012, pp. 2025–2034.

[Collibra] The Internet of Things (IoT): Managing the data tsunami. [Online]. Available: https://www.collibra.com/us/en/blog/the-internet-of-things-iot-managing-the-data-tsunami (last visited: Apr. 25, 2022).

[Cou19] H. R. Council. «Surveillance and human rights - report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression». (2019), [Online]. Available: https://www.ohchr.org/en/HRBodies/HRC/RegularSessions/Session41/Documents/A__HRC__41__35.docx (last visited: Jun. 6, 2022).

[CPMG19] L. Ciechanowski, A. Przegalinska, *et al.*, «In the shades of the uncanny valley: An experimental study of human–chatbot interaction», *Future Generation Computer Systems*, vol. 92, pp. 539–548, Mar. 2019.

[CSGK17] N. Cila, I. Smit, *et al.*, «Products as Agents: Metaphors for Designing the Products of the IoT age », in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, May 2017, pp. 448–459.

[Dat20] Datatilsynet. «Personvernundersøkelsen 2019/2020». (2020), [Online]. Available: https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/personvernundersokelsen-20192020/?fbclid=IwAR03F3dnveTK3Fj-r-PNCZh__z9TAzML7GIBY7YaS2Qr8jl2__ngy8eAbuj0s (last visited: Apr. 5, 2022).

[DDA+20] G. Di Francia, C. Di Natale, *et al.*, Eds., *Sensors and Microsystems*. Cham: Springer International Publishing, 2020, vol. 629.

[Dit19] H. Ditlefsen. «Bruker seks timer av fritida på skjerm». (2019), [Online]. Available: https://www.nrk.no/sorlandet/bruker-seks-timer-av-fritida-pa-skjerm-1.14535434 (last visited: Apr. 25, 2022).

[EBH+19] P. Emami-Naeini, S. Bhagavatula, *et al.*, «Privacy expectations and preferences in an IoT world», in *Proceedings of the 13th Symposium on Usable Privacy and Security, SOUPS 2017*, USENIX Association, 2019, pp. 399–412.

[eco20] T. economist. «The pandemic could give way to an era of rapid productivity growth». (2020), [Online]. Available: https://www.economist.com/finance-and-economics/2020/12/08/the-pandemic-could-give-way-to-an-era-of-rapid-productivity-growth (last visited: May 4, 2022).

[Est17] A. Esteve, «The business of personal data: Google, Facebook, and privacy issues in the EU and the USA», *International Data Privacy Law*, vol. 7, no. 1, pp. 36–47, Feb. 2017.

[FSMR21] N. Ferry, H. Song, *et al.*, *Devops for trustworthy smart iot systems*, 2021.

[Fur22] D. Furszyfer Del Rio, «Smart but unfriendly: Connected home products as enablers of conflict», *Technology in Society*, vol. 68, p. 101 808, Feb. 2022.

[GBR08] J. Gumbis, V. Bacianskaite, and J. Randakeviciute, «Do human rights guarantee autonomy?», *Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol*, no. 62, pp. 77–93, 2008.

[GC22] R. Garg and H. Cui, «Social Contexts, Agency, and Conflicts: Exploring Critical Aspects of Design for Future Smart Home Technologies», *ACM Transactions on Computer-Human Interaction*, vol. 29, no. 2, pp. 1–30, Apr. 2022.

[Gooa] Google. «Digital wellbeing». (), [Online]. Available: https://wellbeing.google/ (last visited: May 29, 2022).

[Goob] ——, «Great technology should improve life, not distract from it». (), [Online]. Available: https://wellbeing.google/our-commitment/ (last visited: May 29, 2022).

[Gua17] T. Guardian, 'Tsunami of data' could consume one fifth of global electricity by 2025, 2017. [Online]. Available: https://www.theguardian.com/environment/2017/dec/11/tsunami-of-data-could-consume-fifth-global-electricity-by-2025 (last visited: Apr. 25, 2022).

[Hon20] S. Hongladarom, «Shoshana Zuboff, The age of surveillance capitalism: the fight for a human future at the new frontier of power», *AI & SOCIETY*, Nov. 2020.

[IEC20] IEC, *Iot 2020: Smart and secure iot platform*, 2020.

[JTK07] G. J. Skulmoski, F. T. Hartman, and J. Krahn, «The Delphi Method for Graduate Research», *Journal of Information Technology Education: Research*, vol. 6, pp. 001–021, 2007.

[Jul22] E. A. Julie Haugen Egge. «Depresjon og angst blant unge i Norge har doblet seg de siste ti årene». (2022), [Online]. Available: https://www.nrk.no/trondelag/hunt_-44-prosent-av-tenaringsjenter-i-norge-plages-av-stress_-angst-og-tunge-tanker-1.15993034 (last visited: Jun. 15, 2022).

[JV17] D. G. Johnson and M. Verdicchio, «AI Anxiety», *Journal of the Association for Information Science and Technology*, vol. 68, no. 9, pp. 2267–2270, Sep. 2017.

[JWJ+12] H. Jia, M. Wu, *et al.*, «Balancing human agency and object agency», in *Proceedings of the 2012 ACM Conference on Ubiquitous Computing - UbiComp '12*, New York, New York, USA: ACM Press, 2012.

[Kar21] A. Karale, «The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws», *Internet of Things*, vol. 15, p. 100 420, Sep. 2021.

[Kim16] K. J. Kim, «Interacting Socially with the Internet of Things (IoT): Effects of Source Attribution and Specialization in Human-IoT Interaction», *Journal of Computer-Mediated Communication*, vol. 21, no. 6, pp. 420–435, Nov. 2016.

[KK20] H. Kang and K. J. Kim, «Feeling connected to smart objects? A moderated mediation model of locus of agency, anthropomorphism, and sense of connectedness», *International Journal of Human-Computer Studies*, vol. 133, Jan. 2020.

[KK22] ——, «Does humanization or machinization make the IoT persuasive? The effects of source orientation and social presence», *Computers in Human Behavior*, vol. 129, p. 107 152, Apr. 2022.

[LCC19] J. Lindley, P. Coulton, and R. Cooper, «The IoT and Unpacking the Heffalump's Trunk», in 2019, pp. 134–151.

[LCM14] H. Limerick, D. Coyle, and J. W. Moore, «The experience of agency in human-computer interactions: a review», *Frontiers in Human Neuroscience*, vol. 8, Aug. 2014.

[LH20] J. Li and J.-S. Huang, «Dimensions of artificial intelligence anxiety based on the integrated fear acquisition theory», *Technology in Society*, vol. 63, p. 101 410, Nov. 2020.

[MH12] S. Mennicken and E. M. Huang, «Hacking the Natural Habitat: An In-the-Wild Study of Smart Homes, Their Development, and the People Who Live in Them», in 2012, pp. 143–160.

[MPA19] 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. 139–154, Jan. 2019.

[MPK+20] K. Marky, S. Prange, *et al.*, «"You just can't know about everything": Privacy Perceptions of Smart Home Visitors», in *19th International Conference on Mobile and Ubiquitous Multimedia*, New York, NY, USA: ACM, Nov. 2020.

[MVS+20] K. Marky, A. Voit, *et al.*, «"I don't know how to protect myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments», in *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, New York, NY, USA: ACM, Oct. 2020, pp. 1–11.

[MW05] J. McCarthy and P. Wright, «Putting 'felt-life' at the centre of human–computer interaction (HCI)», *Cognition, Technology & Work*, vol. 7, no. 4, pp. 262–271, Nov. 2005.

[Nah07] E. Nahmias, «Autonomous agency and social psychology», in Jan. 2007, pp. 169–185.

[NDM01] M. J. Noom, M. Deković, and W. Meeus, «Conceptual Analysis and Measurement of Adolescent Autonomy», *Journal of Youth and Adolescence*, vol. 30, no. 5, pp. 577–595, Oct. 2001.

[Oat06] B. J. Oates, *Researching information systems and computing.* SAGE Publications, 2006.

[PBS+18] X. Page, P. Bahirat, *et al.*, «The Internet of What?», *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 2, no. 4, pp. 1–22, Dec. 2018.

[Rai18] J. M. Raian Ali Emily Arden-Close. «Digital addiction: How technology keeps us hooked». (2018), [Online]. Available: https://theconversation.com/digital-addiction-how-technology-keeps-us-hooked-97499 (last visited: May 30, 2022).

[Rob11] C. Robson, *Real world research.* Wiley, 2011, vol. Third edition, pp. 18–30.

[Row] E. Rowley. «What is matter? the new smart home standard explained». (), [Online]. Available: https://www.techadvisor.com/news/digital-home/what-is-matter-3813815/ (last visited: May 31, 2022).

[Sch19] B. Schmitt, «From Atoms to Bits and Back: A Research Curation on Digital Technology and Agenda for Future Research», *Journal of Consumer Research*, vol. 46, no. 4, pp. 825–832, Dec. 2019.

[Sch20] ——, «Speciesism: an obstacle to AI and robot adoption», *Marketing Letters*, vol. 31, no. 1, pp. 3–6, Mar. 2020.

[SF20] B. K. Sovacool and D. D. Furszyfer Del Rio, «Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies», *Renewable and Sustainable Energy Reviews*, vol. 120, p. 109 663, Mar. 2020.

[Shi20] M. Shitindo, «Restriction of Fundamental Rights in a Context of Emergency: COVID-19 and the Aspect of Autonomy – Can Autonomy Be Limited?», *SSRN Electronic Journal*, 2020.

[Ski96] E. A. Skinner, «A guide to constructs of control.», *Journal of Personality and Social Psychology*, vol. 71, no. 3, pp. 549–570, 1996.

[SN07] J. Seyama and R. S. Nagayama, «The Uncanny Valley: Effect of Realism on the Impression of Artificial Human Faces», *Presence: Teleoperators and Virtual Environments*, vol. 16, no. 4, pp. 337–351, Aug. 2007.

[SSA+19] C. Stephanidis, G. Salvendy, *et al.*, «Seven HCI Grand Challenges», *International Journal of Human–Computer Interaction*, vol. 35, no. 14, pp. 1229–1269, Aug. 2019.

[Svdh18] F. Santoni de Sio and J. van den hoven, «Meaningful human control over autonomous systems: A philosophical account», *Frontiers in Robotics and AI*, vol. 5, p. 15, Feb. 2018.

[Tel22] Telenor. «Iot prediction report 2022». (2022), [Online]. Available: https://www.telenorconnexion.com/wp-content/uploads/2022/03/IoT-Prediction-report-2022_Telenor-IoT.pdf (last visited: May 2, 2022).

[Tjo21] A. Tjora, *Kvalitative forskningsmetoder i praksis.* Gyldendal, 2021, vol. 4.

[TL20] H. Toivonen and F. Lelli, *Agency in human-smart device relationships: An exploratory study*, Sep. 2020.

[TP12] O. Tene and J. Polonetsky, «Big data for all: Privacy and user control in the age of analytics», *Northwestern Journal of Technology and Intellectual Property*, vol. 11, Sep. 2012.

[Unia] E. Union. «Eu legislation in progress - artificial intelligence act». (), [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf (last visited: Jun. 5, 2022).

[Unib] ——, «The digital services act package». (), [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (last visited: Jun. 5, 2022).

[WNC19] M. Williams, J. R. Nurse, and S. Creese, «(Smart)Watch Out! encouraging privacy-protective behavior through interactive games», *International Journal of Human-Computer Studies*, vol. 132, pp. 121–137, Dec. 2019.

[Yri21] I. H. Yri, «Do iot applications have enough focus on user empowerment and agency?», Project Topic Paper, NTNU, Nov. 2021.

[ZGM+19] V. Zimmermann, P. Gerber, *et al.*, «Assessing Users' Privacy and Security Concerns of Smart Home Technologies», *i-com*, vol. 18, no. 3, pp. 197–216, Nov. 2019.

[ZMR17] E. Zeng, S. Mare, and F. Roesner, «End User Security and Privacy Concerns with Smart Homes», pp. 65–80, Jul. 2017.

Appendix A
NSD application and confirmation

The next page contains the approval on the NSD application.

Meldeskjema / Stakeholders perception of agency in a Smart Home contex / Vurdering

Vurdering

Referansenummer
483409

Prosjekttittel
Stakeholders perception of agency in a Smart Home contex

Behandlingsansvarlig institusjon
Norges teknisk-naturvitenskapelige universitet / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Prosjektansvarlig
Katrien De Moor

Student
Inger Helen Yri

Prosjektperiode
17.01.2022 - 13.06.2022

Meldeskjema

Dato	**Type**
17.03.2022	Standard

Kommentar

OM VURDERINGEN
Personverntjenester har en avtale med institusjonen du forsker eller studerer ved. Denne avtalen innebærer at vi skal gi deg råd slik at behandlingen av personopplysninger i prosjektet ditt er lovlig etter personvernregelverket.

Personverntjenester har nå vurdert den planlagte behandlingen av personopplysninger. Vår vurdering er at behandlingen er lovlig, hvis den gjennomføres slik den er beskrevet i meldeskjemaet med dialog og vedlegg.

DEL PROSJEKTET MED PROSJEKTANSVARLIG
For studenter er det obligatorisk å dele prosjektet med prosjektansvarlig (veileder). Del ved å trykke på knappen «Del prosjekt» i menylinjen øverst i meldeskjemaet. Prosjektansvarlig bes akseptere invitasjonen innen en uke. Om invitasjonen utløper, må han/hun inviteres på nytt.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til den datoen som er oppgitt i meldeskjemaet.

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake.

Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER
Personverntjenester vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om:

- lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen
- formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke behandles til nye, uforenlige formål
- dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
- lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER

Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), og dataportabilitet (art. 20).

Personverntjenester vurderer at informasjonen om behandlingen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.

Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER

Personverntjenester legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

Ved bruk av databehandler (spørreskjemaleverandør, skylagring eller videosamtale) må behandlingen oppfylle kravene til bruk av databehandler, jf. art 28 og 29. Bruk leverandører som din institusjon har avtale med.

For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og/eller rådføre dere med behandlingsansvarlig institusjon.

MELD VESENTLIGE ENDRINGER

Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til oss ved å oppdatere meldeskjemaet. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilke type endringer det er nødvendig å melde: https://www.nsd.no/personverntjenester/fylle-ut-meldeskjema-for-personopplysninger/melde-endringer-i-meldeskjema

Du må vente på svar fra oss før endringen gjennomføres.

OPPFØLGING AV PROSJEKTET

Personverntjenester vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!

Appendix B
Consent form - Norwegian

The next page contains the Norwegian consent form that was sent to the Norwegian speaking participants.

Samtykkeskjema - Undersøkelse av Smart Hjem IoT design

Informasjon om prosjektet

Du blir invitert til å delta i et forskningsprosjekt som handler om å undersøke designet av smart hjem teknologi og hvordan teknologien bør utvikles for å tilfredsstille menneskelige behov og tilfredshet. I dette skrivet gir vi deg informasjon om bakgrunn og formål for prosjektet, samt hva deltakelse i prosjektet innebærer.

Formålet med prosjektet

Prosjektet har som formål å undersøke designet av smart hjem teknologi, fra idé til sluttprodukt. Samt undersøke om det er korrespondanse mellom designmetode og menneskelige behov og ønsker. Målgruppen består av et ekspertpanel med personer fra industri, akademia og personer med politisk og statlig syn på smart hjem teknologi. Grunnen for valget av målgruppe er fordi disse synspunktene gir et bredt kunnskapsspekter på temaet og kan bidra med kunnskap som kan være nyttig for videre forskning.

Hvem er ansvarlig for prosjektet?

Dette prosjektet inngår i en masteroppgave i Kommunikasjonsteknologi og digital sikkerhet ved Norges teknisk-naturvitenskapelige universitet (NTNU). Masterstudent Inger Helen Yri og førsteamanuensis Katrien De Moor fra Institutt for informasjonssikkerhet og kommunikasjonsteknologi ved NTNU er ansvarlig for prosjektet.

Hva innebærer deltakelsen i prosjektet for deg?

Deltakelse i studien betyr at du deltar i et intervju, som tas opp (lydopptak ved fysisk møte eller videoopptak ved digitalt møte) med varighet på maksimalt 45 minutt. Det kan også være aktuelt å svare på en kort spørreundersøkelse eller et par oppfølgingsspørsmål i ettertid av intervjuet, dersom du har tid eller mulighet. Du får et supergavekort (verdi 200 kr) som insentiv for deltakelsen i studien.

Frivillig deltakelse og mulighet for å trekke deg

Deltakelse i prosjektet er frivillig. Ved å fylle ut og sende inn dette skjemaet, samtykker du i å delta i studien. Du kan trekke tilbake samtykket ditt uten noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Alle lydopptak slettes så fort intervjuet er transkribert og senest 13.juni 2022. I tillegg ber jeg om tillatelse til å få kategorisere ditt perspektiv innenfor en av følgende kategorier: Industri-perspektiv, akademisk-perspektiv, politisk-perspektiv eller statlig-perspektiv. All annen data vil være anonymisiert.

Dine rettigheter

Så lenge du kan identifiseres i datamaterialet, har du rett til:

- Innsyn i hvilke personopplysninger som er registrert om deg, og å få utlevert kopi av opplysningene.

- Sletting og ev. endringer av dine personopplysninger.
- Klage til Datatilsynet om behandlingen av dine personopplysninger.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke. På oppdrag fra NTNU har Norsk senter for forskningsdata (NSD) vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket (prosjektID: 483409)

Hvor kan jeg finne ut mer?

Hvis du har spørsmål til studien eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- NTNU v/ Katrien De Moor, katrien.demoor@ntnu.no
- Vårt personvernombud Thomas Helgesen, thomas.helgesen@ntnu.no

Sideskift

Jeg har mottatt og forstått informasjonen om prosjektet "Undersøkelse av Smart Hjem IoT design" og fått anledning til å stille spørsmål. Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet.

Jeg samtykker...

Å delta på intervju med lydopptak (ved fysisk møte), inkl. besvarelse av et par korte spørsmål i dette skjemaet.

Å delta på intervju via Zoom med videoopptak, inkl. besvarelse av et par korte spørsmål i dette skjemaet.

Appendix C
Consent form - English

The next page contains the English consent form that was sent to the English speaking participants.

Consent form - Investigating the Smart Home IoT design process

Side 1

Information about the project

You are invited to this research project about the investigation of the design process of smart home IoT and how the technology should be designed to ensure humans' well-being and satisfaction. In this form, there will be general information about the background and purpose of this project, as well as what participation in this project will involve.

Purpose of the project

This project's purpose is to investigate the smart home IoT design, from idea to end product. As well as discover if there is an established correspondence between the design method and humans' needs and wishes. The target audience consists of an expert panel, including people from the industry, academia as well as persons with the political and governmental perceptions of smart home IoT. The reasoning for this selection is that these perspectives give an overview and a broader knowledge of the topic. Their perspective can also give broader knowledge that can be highly valuable in further research on the topic.

Who is responsible for the project?

This project is part of a master's thesis in Communication Technology and Digital Security at the Norwegian University of Science and Technology (NTNU). Master student Inger Helen Yri and associate professor Katrien De Moor from the department of Information Security and Communication Technology at NTNU are responsible for this project.

What does participation in this project involve?

Participation in this study involves an interview that will be recorded (video recording) with a duration of a maximum of 45 minutes. It may also be relevant to answer some follow-up questions in retrospect of the interviews if you have the time or opportunity. You will receive a gift card (NOK 200) as an incentive for participation in the study.

Voluntary participation and the opportunity to withdraw

By filling out and submitting this form, you agree to participate in the study. You can withdraw your consent for no reason. All your personal information will then be deleted. It will not have any negative consequences for you if you do not want to participate or later choose to withdraw.

What happens to your information when we end the research project?

All audio recordings are deleted as soon as the interview has been transcribed and no later than 13 June 2022. In addition, I ask permission to categorize your perspective within one of the following categories: Industry-perspective, academic-perspective, political-perspective or government-perspective. All other data will be anonymized.

Your rights

As long as you can be identified in the data material, you have the right to:

- Access to which personal information is registered about you, and to receive a copy of the information.
- Deletion and possibly changes to your personal information.
- Complaint to the Norwegian Data Protection Authority about the processing of your personal data.

What gives us the right to process personal data about you?

We process information about you based on your consent. On behalf of NTNU, the Norwegian Center for Research Data (NSD) has assessed that the processing of personal data in this project is in accordance with the privacy regulations (project ID: 483409)

Where can I find more information?

If you have questions about the study or want to exercise your rights, please contact:

- NTNU v/ Katrien De Moor, katrien.demoor@ntnu.no
- Our privacy representative Thomas Helgesen, thomas.helgesen@ntnu.no

Sideskift

Side 2

I have received and understood the information about the project "Investigating the Smart Home IoT design process" and had the opportunity to ask questions. I agree that my information will be processed until the project is completed.

I consent ...

To participate in an interview with audio recording (by physical meeting), including answering a few short questions in this form.

To participate in an interview on Zoom with video recording, including answering a few short questions in this form.

Appendix D
Interview guide in Norwegian

The next page contains the Norwegian interview guide including the structure and the questions asked in the interviews.

Intervjuguide

Målgruppe: Eksperter innenfor smart hjem teknologi

Tidsramme: 30-40 min

Introduksjon:

- Hei, først så setter jeg veldig pris på at du har tatt deg tid til denne samtalen.
- Har du noen spørsmål til samtykkeskjemaet jeg sendte ut?
    - Nei:
        - OK, da starter jeg opptaket
    - Ja:
        - Svarer på spørsmål
- Kort introduksjon om intervjuer
- Kort om formålet med samtalen
- Om jeg stiller et spørsmål som du av ulike grunner ikke kan svare på, er det bare å si ifra om dette så går vi bare videre

Oppvarming:

- Så da lurte jeg litt på om du hadde lyst til å fortelle kort hva du har jobbet med relatert til smart hjem?

Hoveddel:

Bolk 1 – Fordeler og ulemper:

- Hva anser de som de viktigste fordelene og utfordringene med IoT?
    - Smart hjem?
    - Hvorfor?
    - Eksempel?

Bolk 2 - Formål/Mål:

- Hvorfor er IoT løsninger nyttige, for hvem?
    - Tror du det er folk/grupper det kan være skadelig for?
        - Hvorfor/Hvorfor ikke?
    - Hvordan oversetter man dette teknisk
    - Hvilke suksesskriterier må stilles?

Bolk 3 – Prosess:

- Hvilke reguleringer må man ta stilling til i utviklingen av Smart IoT produkt?

    - Hvilke reguleringer er på plass for å beskytte vanlige folk i en smart hjem kontekst?
- Finnes det en prosess der nye smart produkter blir undersøkt før de kommer på det norske markedet?
    - Sertifiseringskrav?
    - Hvilke kriterier stilles?
    - Blir alle smart produkt «behandlet likt» mtp. regulering de må gjennom, eller er det produkter som må gjennom mer regulering enn andre? (feks. der sensitiv informasjon blir samlet inn ol.)
- Er det mye standardisering for smart hjem løsninger?
- Hvordan sikrer dere brukervennlighet i produktene?
    - Har dere en teknisk prosess/test prosess som evaluerer om suksesskriteriene er opprettholdt?
    - Hvordan blir dette testet i brukertester?
    - Hva er viktigst for dere å teste i brukertester?
    - Hvordan løser dere human-centric behovet teknisk?
    - Hvordan sikrer dere at personvern er i varetatt?
- AI er kjent for å lære av brukerdata for å kunne optimaliseres, hvordan funker dette i praksis? Hva skjer med dataen?
    - Hadde det vært mulig å holde dataen lokalt?
- Hvordan sikrer du tillit til IoT løsningen/systemet?
    - Hva legger du i begrepet tillit?
    - Hvem er tillitt viktigst for og hvorfor?
    - Hvem må beskyttes? Hvorfor?
    - Inkluderer det individets autonomi?
    - Hva tenker du når du hører begrepet autonomi?
- Nylig i litteraturen blir ofte autonomi nevnt, har du kjennskap til begrepet?
    - Hvordan tenker du på dette i en smart hjem kontekst?
    - Har dere dette på agendaen?
        - Nei:
            - Ser du noen risikoer med å ikke ha det?
        - Ja:
            - Hvordan jobber dere med dette?
            - Hvordan sikrer dere at personlig autonomi er beskyttet?
            - Hvordan oversetter man dette teknisk?

Bolk 4 – Konsekvens/ risiko:

- Generelt i smart hjem, ser du noen konsekvenser/risikoer for mennesker og samfunn
    - Hvorfor
    - Konkret eksempel
    - Jobbere dere med dette?

    - Hvordan har dere det på agendaen?
  - Hvilke positive eller evt. negative konsekvenser er det å ha et fult integrert smart hus/ smart hus med mange komponenter?

Avslutning:

- Har du noe mer du vil legge til eller spørsmål du skulle ønske jeg spurte om?
- Tusen takk for deltagelsen!

Appendix E
Interview guide in English

The next page contains the English interview guide including the structure and the questions asked in the interviews.

Interview guide

Target group: Experts in smart home technology

Time frame: 30-40 min

Introduction

- I really appreciate that you took the time to contribute!
- Do you have any question about the consent form I sent you beforehand?
  - No:
    - Start the recording
  - Yes:
    - Answer questions
- Introduction about the interviewer
- Short about the purpose of the interview and project
- If I ask questions that you for various reasons can not answer, just let me know and we will just move on to the next question

General about the expert

- First, can you tell me a little bit about what you have worked on related to smart home technology?

Main section

Topic 1 – Pros and cons

- What do you consider to be the most important benefits and challenges of IoT?
  - Smart Home?
  - Why?

Topic 2 – Purpose/goal

- Why is IoT solution useful and for whom?
  - Do you think it is people or groups IoT can be harmful for?
  - How do we evaluate this in the development of the product?
  - What success criteria must be set?

Topic 3 – Process

- *Do you have knowledge of how smart products are developed / the process?*

    - *Regulations?*
    - *User testing?*
- *What regulations must be considered in the development of Smart IoT product?*
    - *What regulations are in place to protect ordinary people in a smart home context?*
    - *How should this be evaluated/guaranteed in the development process?*
- *Is there a process where new smart products are examined before they enter the Norwegian market?*
    - *What criteria are set?*
    - *Are all smart products "treated equally" when it comes to regulation they have to go through, or are there products that must go through more regulation than others? (e.g., where sensitive information is collected, etc.)*
- *How do the user tests work?*
    - *Do you have a technical process / test process that evaluates whether the success criteria have been maintained?*
- *What do you consider to be the biggest gaps in today's development of IoT solution?*
    - *Is there standardization when it comes to development of IoT?*
        - *Do you think it is enough standardization in IoT?*
- *Do you think that majority of today's smart home devices succeed in protecting human users?*
    - *Why/why not?*
    - *If no:*
        - *What do you believe needs to be done in the development process?*
- *What do you experience that the EU has the most focus on in the IoT or Smart Home context?*
- How do we/or the industry ensure trust in the IoT solutions?
    - What do you put in the concept of trust?
    - Who is trust most important for and why?
    - Who needs to be protected? Why?
    - Do you think certification solution can help bring more trust to smart home solution?
    - Is it in theory possible to make AI IoT systems, where the data only is local, i.e., do not leave the house?
    - Does it include the autonomy of the individual?
- Do you have any thoughts on agency and autonomy in a Smart Home context?
    - Why/why not?
    - Can you elaborate?
    - Has this been a topic of interest in your field of expertise?
    - When AI is integrated into the products, do you see any challenges to that related to personal autonomy/agency?

Topic 4 – Consequence / risk

- *If we take a look on smart homes in general, do you see some consequences / risks for people and society?*
    - Why?
    - Do you have an example?
    - Is this something you work with?
    - How is this on the agenda?
- *What are the positive or possibly negative consequences of having a fully integrated smart house / smart house with many components?*

End:

- *Do you have anything more you want to add or questions you wish I asked?*
- *Thank you so much for participating!*

Appendix F
The transcribed material

The transcribed material is not included in the appendix since it required significant editing in order to ensure the anonymity of the participants, enterprise, and legal/policy institutions. So to ensure that this master thesis' does not lead to any kind of disclosure of sensitive information it was considered that it should be excluded. However, it is possible to ask to view the fully anonymous transcribed material on request.

NTNU

Norwegian University of
Science and Technology