Silje Kløften Lein

Exploring the Enablers and Barriers of Human Autonomy in IoT

Master's thesis in Communication Technology and Digital Security
Supervisor: Katrien De Moore
Co-supervisor: Kaja Fjørtoft Ystgaard
August 2023

Master's thesis

NTNU
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

Silje Kløften Lein

Exploring the Enablers and Barriers of Human Autonomy in IoT

Master's thesis in Communication Technology and Digital Security
Supervisor: Katrien De Moore
Co-supervisor: Kaja Fjørtoft Ystgaard
August 2023

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

Title: Exploring the Enablers and Barriers of Human Autonomy in IoT
Student: Lein, Silje Kløften

Problem description:

The rapid growth of the Internet of Things (IoT) has led to an increased integration of technology in our daily lives. While this technology brings about many benefits, it also poses significant challenges, particularly in the area of human autonomy. As we rely more and more on connected devices, it is essential to ensure that they do not compromise our ability to make decisions and control our own lives. While there is a focus in the literature on factors and requirements that may facilitate human autonomy, the relevant insights in this respect are rather scattered across different fields. Moreover, existing technical solutions to embed these to date still seem scarce and insufficient. For instance, proposed ethical standards and guidelines to incorporate human autonomy exist [MTB22; Spi18], but few standards specify how to translate meaningful human autonomy to be implemented technically [YD23]. This poses a significant challenge for the development of future network technologies that strive to be truly human-centric. In addition, the lack of a common understanding of the definition of human autonomy and what it implies for the IoT makes technical interpretations inconsistent when they are based on different perspectives of the term. So, an important first step would be to establish such an understanding.

The aim of this thesis is to explore factors that enable and inhibit human autonomy in the IoT, and to examine their significance for ensuring human autonomy in future network technology. To achieve this objective, the study will use a two-part methodology consisting of a literature review and a Delphi method-inspired survey (further referred to as Delphi survey). The literature review will aim to map current main technical and non-technical factors that enable and inhibit human autonomy in the IoT. Depending on the results of the review, a use case within the IoT will be determined, on which the Delphi survey will focus. A Delphi survey is often performed to gain consensus on topics where there are multiple perspectives, complexity, and diverging opinions. In this case, such a survey can be useful for achieving a more objective perspective on what it means to be truly human-centric, as well as how to technically implement human autonomy in the IoT.

The use case will define what is to be investigated technically in the survey. Then, the Delphi survey will collect qualitative data from experts and stakeholders to identify the significance of these factors in the future. The research question that will guide the survey is as follows: To what degree may the technical and non-technical factors identified in the literature facilitate human autonomy in future design and use of IoT devices? By exploring this question, the study aims to provide insights, from a multi-disciplinary perspective, into factors that are critical for ensuring human autonomy in the IoT, and to offer recommendations for further research on future network technology and how we can make it truly human-centric.

Approved on:	2023-03-24
Main supervisor:	Associate Professor De Moor, Katrien, NTNU
Co-supervisor:	Ystgaard, Kaja, NTNU

Abstract

With the realization of the Internet of Things (IoT), humans are surrounded by digital technology in their everyday lives. The technology has begun to assume control over different tasks, including the fulfillment of societal needs. While this technology brings about many benefits, it also poses significant challenges, particularly in the area of human autonomy. As humans rely more and more on connected devices, it is essential to ensure that these devices do not compromise peoples' ability to make decisions and control their own lives. Technical solutions exist that try to implement protection of autonomy in various degrees, but they appear insufficient. Additionally, the lack of a common understanding of autonomy presents a challenge because it leads to discrepancies in technical interpretations based on different perceptions of the term.

This research aims to explore factors that enable and inhibit human autonomy in IoT and examine their significance for ensuring human autonomy in future network technology. In addition, an attempt is made to categorize varying definitions of autonomy from the perspective of experts and the public view. For this purpose, a two-part methodology has been applied, consisting of a systematic literature review followed by two Delphi method-inspired surveys. In total, 12 experts and 123 end-users were queried. 41 articles were analyzed in the review to identify possible factors, whereupon the factors were utilized to create the two surveys. The surveys aimed to assess these factors and their importance for autonomy in future IoT, as well as categorize perceptions of autonomy.

The findings from the literature review suggest that while some factors are distinct barriers or enablers, determining whether a factor is an enabler or a barrier can often be two sides of the same coin. Moreover, when compared to the findings from the surveys, it can seem like current literature has focused mostly on protecting what is defined in this thesis as personal autonomy or "freedom to" (perform actions), and not so much political autonomy or "freedom from" (external influences). The experts' assessment of factors implies that some of the current solutions that are said to be enablers of autonomy may not fulfill their purpose effectively, even though end-users seem to have more faith in these. Finally, important barriers to human autonomy are the devices' potential for mass-surveillance, and systemic biases in how IoT services are provided. With this thesis, the hope is to contribute towards research on how to make future network technology truly human-centric.

Sammendrag

Realiseringen av tingenes internett (IoT) har gjort at mennesker er omgitt av digital teknologi i hverdagen. Denne teknologien blir tildelt ansvar for ulike oppgaver, blant annet funksjoner som skal fylle samfunnsbehov. Selv om IoT-teknologien gir mange fordeler, bringer den også betydelige utfordringer, spesielt for hvordan mennesker kan utøve sin autonomi. Ettersom samfunnet og menneskene som bor i det blir mer og mer avhengige av digitale teknologier, blir det viktig å sikre at disse ikke kompromitterer folks evne til å ta egne avgjørelser og kontrollere sine liv. Det finnes tekniske løsninger som forsøker å implementere en form for beskyttelse av autonomi, men disse framstår som utilstrekkelige. I tillegg utgjør mangelen på en felles forståelse av autonomi en utfordring, da dette fører til uoverensstemmelser i tekniske tolkninger basert på ulike oppfatninger av begrepet. Målet med denne masteroppgaven har vært å utforske faktorer som muliggjør eller hindrer menneskelig autonomi i IoT, samt å undersøke disse faktorenes viktighet for å sikre autonomi i fremtidig nettverksteknologi. I tillegg er det gjort et forsøk på å kategorisere ulike betydninger av begrepet autonomi blant eksperter og sluttbrukere. Til dette formålet er det benyttet en todelt metodikk bestående av en systematisk litteraturstudie etterfulgt av to Delphi-metodeinspirerte spørreundersøkelser. Totalt deltok henholdsvis 12 eksperter og 123 sluttbrukere i disse undersøkelsene. 41 artikler ble analysert i litteraturstudiet for å identifisere mulige faktorer, hvorpå faktorene ble benyttet til å lage de to undersøkelsene. Hensikten med undersøkelsene var å evaluere faktorene og deres betydning for autonomi i fremtidig IoT, samt kategorisere ulike oppfatninger av autonomi. Funnene fra litteraturstudien tyder på at selv om noen faktorer er distinkte drivere og barrierer, kan det å bestemme om en faktor er en driver eller en barriere ofte være to sider av samme sak. Videre, dersom man sammenligner med funnene fra undersøkelsene, kan det virke som om eksisterende litteratur hovedsakelig har fokusert på å beskytte det som i denne oppgaven defineres som personlig autonomi eller «frihet til» (å utføre handlinger), og ikke så mye på politisk autonomi eller «frihet fra» (ytre påvirkninger). Ekspertenes vurdering av faktorene tilsier at noen av dagens løsninger som sies å være drivere av autonomi ikke nødvendigvis oppfyller formålet hensiktsmessig, selv om sluttbrukerne ser ut til å ha større tro på disse. Til slutt er viktige barrierer mot menneskelig autonomi IoT-enhetenes potensiale for masseovervåkning, samt systemiske skjevheter i hvordan IoT-tjenester leveres. Med denne oppgaven er håpet å bidra til forskning på hvordan man kan gjøre fremtidens nettverksteknologi virkelig menneskesentrert.

Preface and Acknowledgements

This master's thesis is submitted to meet the requirements for a Master of Science (MSc) degree in Communication Technology and Digital Security at the Department of Information Security and Communication Technology (IIK) in the Norwegian University of Science and Technology (NTNU). The research was carried out between February and August 2023, and the project has been supervised by Kaja Fjørtoft Ystgaard and Katrien De Moore.

I would like to extend a warm thank you to my supervisors Kaja and Katrien for helping me throughout the semester. Kaja has given tremendous time and dedication to the supervision. With her professional knowledge in this field and her ability to give relevant input in all stages of the process she has been instrumental in shaping this thesis. Katrien has a vast repertoire of knowledge, and always knows how to explain the most complicated things in a simple manner. She has been very helpful in giving advice and guidance in times of need.

Also, a very big thank you to my mom, Kirsti Lein, who has been my personal motivator (and chauffeur) in the last weeks of writing. Lastly, I would like to thank my boyfriend, my friends, and the rest of my family for putting up with me and supporting me over the past few years.

Contents

Appendices

List of Figures

List of Tables

List of Acronyms

AAL Ambient Assisted Living.

ABC Agent-based Computing.

ABE attribute-based encryption.

AI Artificial Intelligence.

AmI Ambient Intelligence.

ARCS Adaptive Remote Control System.

CEP Complex event processing.

ForSTI Foresight for Science, Technology and Innovation.

GDPR General Data Protection Regulation.

H2M human-to-machine.

HCD Human-Centered Design.

HCI Human-Computer Interaction.

HIoT Healthcare Internet of Things.

ICT information and communications technology.

IoMT Internet of Medical Things.

IoT Internet of Things.

ISTAG Information Society Technologies Advisory Group.

IT Information technology.

M2M machine-to-machine.

MAS Multi Agent Systems.

MTKOM Communication Technology and Digital Security.

NTNU Norwegian University of Science and Technology.

PDS Personal Data Store.

PPRS privacy preference recommender system.

RFID Radio Frequency Identification.

SDT Self-Determination Theory.

Chapter 1 Introduction

In a rapidly evolving world, understanding the role humans have in future technological developments is principal. This study addresses how to ensure human autonomy in the future of Internet of Things, seeking to understand how autonomy is interpreted and translated technically, as well as identifying the main enablers and barriers to autonomy in the IoT. Through a systematic literature review, relevant literature has been investigated to identify current factors that impact autonomy in IoT. The resulting factors were used to create two surveys, where the aim was to validate the findings from the review, and assess the factors' significance as enablers and barriers of autonomy in future IoT. The surveys also attempted to categorize different perceptions of the term human autonomy among experts and end-users. By exploring the enablers and barriers of autonomy, as well as various perspectives on the term, this research aims to shed light on what needs to be prioritized in the translation of autonomy into the IoT.

1.1 Motivation and Context

With the actualization of the Internet of Things (IoT), humans are surrounded by digital technology in their everyday-lives. The interlinked system of communicating devices can only be anticipated to grow more pervasive in the future, with the projected rise to almost 30 billion connected devices by 2030 [G]. It seems evident that society will integrate these devices extensively, as the vision is a ubiquitous computing paradigm with technology built directly into the environment seamlessly and invisibly [BP06]. The pervasiveness and volume of these devices are of concern to human autonomy [LS21], and regulatory frameworks are struggling to keep up with the dynamic development [BBNT18]. Existing literature indicates that attention is being put towards getting humans to accept this technology [Eco17], but perhaps what is lacking to gain acceptance are specifications on how to translate meaningful autonomy to be implemented technically into the IoT [YD23].

The Internet of Things has many application areas and use cases, both to serve individual needs and societal functions. These include, but are not limited to, wearables, smart cars, machine-to-machine system used in industry and smart homes, healthcare systems, biometrics, retail, smart cities and smart energy [BBNT18; Kar21]. The breadth of these areas underlines the pervasiveness of IoT, and thereby the need to design for human autonomy so humans can control both their personal and public environment [LS21]. Traditionally, technology development has often been driven by the challenge of innovation and the desire to find out is technically possible, without necessarily focusing on serving the needs of humans and society [BP06]. But, if society is going to be permeated by technology, there needs to be a shift towards a more human-centered focus. This thesis argues that IoT researchers and developers have a responsibility to make this happen.

Moreover, certain human traits such as agency, intentionality, awareness, freedom, control over thoughts and actions, and human limits, are at risk of being unlearned if not cultivated and practiced [BBNT18]. To really emphasize this, an analogy will be used, namely the carousel kitten experiment from 1963 [Spi18]. Following is an excerpt from the pre-project [Lei23], where this analogy was first introduced:

> *In [Spi18], Spiekermann compares humans in the world of the IoT to carousel kittens from an experiment conducted by neuroscientists in 1963. The kittens were all raised in the dark, except for being placed in pairs in carousels for three hours per day. In the carousel, they were not able not see each other but still received the same visual stimuli. One of the kittens in each pair was placed in a basket being pulled by the other one, who was allowed to walk freely. In the end, the passive kittens ended up with shortcomings in intelligence and survival ability, while the active kittens had developed normally. Spiekermann compares this to humans passively being steered by IoT technology without any agency of our own. She advocates the need to consider questions such as what humanity will look like in 30 years if humans are treated like passive kittens, and what we can do to avoid this kind of future.*

So, how can humans avoid becoming passive kittens? According to Spiekermann, agency needs to be preserved. This can be extended to apply autonomy as well. Designing for autonomy allows humans to influence and control the personal and public environment [LS21], which would probably be helpful if trapped in a carousel-like contraption, but also in the context of everyday life surrounded by IoT devices. It is therefore of interest to investigate how autonomy is interpreted among various perspectives, to determine how it should protected in the IoT. In relation to this is can also be beneficial to explore the current factors that can be enablers and barriers to autonomy, and investigate how these can potentially contribute to future scenarios where autonomy is preserved or lost.

1.2 Research Questions

The research questions have been adjusted from what was proposed in the pre-project [Lei23]. Instead of determining a specific use case, the research ambitiously tries to address the IoT in general. In addition to attempt to map barriers and enablers of autonomy in current IoT and assess how they can impact future IoT, focus has been on investigating how autonomy is interpreted among experts and end-users. This is all done with the overarching goal of contributing towards the realization of truly human-centered IoT. The following questions have guided the research in this thesis:

- **RQ1**: How can different interpretations of autonomy be categorized among experts and end-users, in an everyday-life context and in an IoT context?
- **RQ2**: What are the existing factors that can be barriers or enablers of human autonomy in the context of the IoT?
- **RQ3**: To what degree may the factors identified in the literature enable or inhibit human autonomy in future design and use of IoT devices?

Research Question 1 addresses various definitions of autonomy that exist. Having different definitions of the term may lead to discrepancies in the conditions that need to be fulfilled to say that full degree of autonomy is accomplished. Prunkl [Pru22] argues that there is a need to establish a common definition to be clear on what the threats to autonomy are, but Dainow argues that this is unnecessary and impossible [Dai17]. Investigating the perceptions of human autonomy among end-users and experts may give insight into which aspects of the term need to be prioritized in the technical translation into IoT.

Research Question 2 is directed at current IoT solutions and how autonomy and related concepts such as empowerment, agency, and control has been taken into account in the technology. By mapping factors from the literature that can be enablers or barriers, the hope is to gain an overview of which solutions have been operationalized and succeeds in addressing human-centric outcomes such as human autonomy, agency, empowerment, and control, as well as barriers that require action taken in order to reach said outcomes.

Since the goal is to build truly human-centered IoT solutions in the future, Research Question 3 was formulated to try and ascertain which of the factors hold most significance in contributing towards a future where human autonomy is either maintained or lost, and thereby should be given attention in future development of IoT. By including the views of both domain experts who possess relevant knowledge about the topic, and laypeople who ultimately will be the end-users of future IoT, this thesis aspires to explore new perspectives on how to ensure human autonomy in future network technology which strives to be truly human-centric.

1.3 Report Outline

The rest of the thesis is structured into five chapters. Relevant background for the thesis research is introduced in Chapter 2. This includes an explanation of technical developments that have aimed to achieve human-centered outcomes, terms and concepts related to the humanistic perspective of autonomy, technical developments that have utilized human-centered theories or principles throughout the design and development processes to reach human-centric goals, and lastly, related and similar research to what has been conducted in this thesis. The methodology, i.e., a systematic literature review and two surveys, is described and justified in Chapter 3. A discussion of method limitations is also included. Chapter 4 illustrates and describes the results from the literature review and the two surveys, and explains how they provide answers to the research questions stated above. The results and their limitations are discussed in Chapter 5. Implications the results may have are debated. Chapter 6, the last chapter, summarizes and concludes the findings, in addition to suggesting further research on the topic.

Chapter 2 Background

The following chapter contains examples of concepts and technical solutions that attempt to address human autonomy, agency, empowerment, and/or control in the IoT ecosystem. Moreover, concepts related to these four terms and the human-centered context are explained. Finally, related works on factors and aspects influencing human autonomy in IoT and similar technology are presented.

However, it is important to acknowledge that the information provided in this chapter is non-exhaustive. The aim is to highlight key points and offer a foundation for understanding the subject matter. For a more comprehensive understanding, interested readers can explore the sources and references presented, which offer additional and detailed information on various aspects of the technical and human-centered contexts of the topic of human autonomy in the IoT.

2.1 The Technical Context

When attempting to protect human-centered interests related to autonomy, agency, empowerment, and control in IoT technology, the technical contributions can be categorized into four feature categories, as presented by Ystgaard et al. [YAP+23]: design framework, architecture, user monitoring, and user interface. Firstly, design frameworks consist of a set of principles and procedures to be followed when designing new technology. Secondly, architecture can be the proposal of novel architectures that have taken human-centered interest into account. Thirdly, user monitoring pertains to functionalities that detect user presence and characteristics, and attempt to adapt their services according to the collected information. Lastly, user interface relates to features for allowing user interaction through more empowering interfaces that are designed to be more accessible, explainable, or easy, or a combination of these qualities.

The following section will present some of the technical concepts that exist, and a subset of solutions and functionalities have been built in an attempt to address autonomy, agency, empowerment, or control, or a combination of one or more of these outcomes. First, selected developments related to user monitoring are introduced, followed by a brief rundown of some works in the architecture category, and lastly, solutions for human interaction with the IoT technology.

2.1.1 User Monitoring Functionality

User monitoring aims to learn about the user's habits as well as the surrounding environment to provide a personalized system service [YAP+23]. An important concept that enables this functionality is context-awareness.

Context-awareness has been a technological driver for the IoT, and refers to a system's capacity for collecting information about the surrounding environment at any time and adapting accordingly [Tec]. A system can be said to be context-aware when it provides the user with relevant information or services, or both, in their task [ADB+99; SGP+20]. In the framework "Ethical Design in the Internet of Things" that aims to empower the user, give control over personal data, and support agency, Baldini et al. [BBNT18] state that support for context should be essential in the relationship between users and the IoT. Given the dynamic nature of contexts, this does, as stated, require constant monitoring of users. For example, through means such as location tracking, recording specific activities like card scanning when the user enters their workplace [BBNT18], keeping track of behaviors, intentions, and preferences collected by IoT devices.

Moreover, personalization as a concept in IoT possesses three fundamental problems to human-centered interests, according to Nolin and Olson [NO16]. These include the constriction of personal development, the assumption that the user has one single identity, and limited recognition of situational differences (i.e., context-awareness). In the following paragraph, a summary is provided of these three issues as explained by Nolin and Olson in [NO16].

When based on historical interests and behaviors, personalization may limit future personal growth. Semantic agents and filtering algorithms may focus on past identities, reaffirming them and filtering out information that reflects other potential identities. This is particularly problematic for young people who need to explore and find evolving maturity through the information they access. Moreover, some technologies are developed with the assumption that each user has only one identity, disregarding the fact that people can assume different roles throughout the day. The emphasis on single identities by technology can push humans to become less complex and more predictable. Lastly, information needs are situated and vary according to specific daily life situations [NO16]. This means that they are context-dependent, which necessitates context-awareness to properly provide the personalized service.

Technical Developments Based on User Monitoring

Recommender systems in IoT are examples of a technical development utilizing collected data about the user and their environment to provide a personalized service. Shanmugarasa et al. [SPKZ21] propose a privacy preference recommender system (PPRS) designed to work within the constraints of the Personal Data Store (PDS) environment. To clarify, a PDS is a technical architecture that aims to enable individuals to collect and curate their personal data, to allow individuals to have more control over their data and preserve their autonomy in a data-driven world [VO14]. Shanmugarasa et al.'s PPRS aims to assist users in making privacy settings for data sharing. The PPRS employs context awareness for the recommending of privacy settings, and claims to operate effectively even with limited data available about the user's privacy preferences. The PDS architecture is used to store data locally, which the PPRS processes to make the recommendations.

Furthermore, Baskar et al. [BLY13] describe the development of a multi-agent dialogue system and the use of the ACKTUS ontology, which contains a basic model of the user and their activities. The purpose is to provide tailored support in an intelligent environment by considering various user traits and adjusting the knowledge accordingly. The system aims to allow the user to have control over the system through human-agent dialogues, which are viewed as a means of providing personalized support. The system uses context-awareness to create an individual environment for the user, taking into account their preferences, activities, and interests to provide personalized assistance.

Another technological advancement in the domain of user monitoring is the emergence of Healthcare Internet of Things (HIoT) devices. These devices specialize in monitoring patients and tracking various health-related data to also allow the patient to self-monitor their disease. In the healthcare sector, a study on the use of HIoT devices among patients with diabetes indicates that the HIoT devices enhance patient empowerment through four dimensions: self-efficacy, patient control, knowledge development, and participation in the decision-making process along with the doctor [FAMC22]. However, Lupton [Lup13] suggests that self-monitoring can be both empowering and disempowering to patients. Here, Lupton argues that for instance, it can disempower the patient by placing the healthcare responsibility on the patient and prioritizing metric data over personal experience.

2.1.2 Architecture and Technical Frameworks

It is possible to try and integrate human-centered interests into the architecture of IoT devices from the beginning, and to build technical frameworks that require various degree of user participation. Examples of technical attempts to this will be provided in the coming paragraphs, along with mechanisms that aim to protect security and privacy in systems.

Information and Communication Security

The subsequent paragraphs will introduce a selection of aspects related to information security in the IoT. While this domain has gained considerable attention in research, it does not serve as the primary focus in this thesis; therefore, only a non-comprehensive assortment of aspects are presented. However, security and privacy are stated as promoting user control and control over the data shared with the IoT system [PZ21; Dim16; JKH20], hence information security is of significance within this context.

More and more devices are being connected to the Internet of Things and communicating amongst each other and over the Internet. Since a lot of this communication is happening without human control [HS20], it is vital that it occurs in a secure manner. An important aspect of securing the information that is being shared, is cryptography. In their IoT cryptography review, Damghani et al. [DHD19] conclude that the current security level is not sufficient for future IoT applications, and that there is a need for a robust cryptosystem. The proposed solution for achieving this in an IoT system with limited resources is with the use of lightweight cryptography [DHD19; RMI22; AAA21; SS22]. Other suggested encryption solutions include a DNA computing based stream cipher [HS20] and attribute-based encryption (ABE) in the Internet of Medical Things (IoMT) networks for secure interaction, analysis, and processing of medical data [PZ21].

Another important security requirement is authentication of users and objects in the network; they are the ones who have access to the data collected by the devices. Authentication in the IoT refers to verifying and ensuring the identity of objects. It is important for each object to posses the capability to identify and authenticate all other objects within the system or the specific part of the system in which it is located [EFCS19]. Singh and Singh [SS22] present a signature-based 3-factor authentication framework to protect the network against unauthorized access by users and rogue devices.

Data Management and Protection

The management and protection of personal data is of interest when protecting human autonomy technically. There are various methods of providing the user with autonomy, that can be labelled as active or passive, or somewhere in between, based on various degree of involvement, control, and user agency. Since the functionalities offered by the developers are the only mechanisms for end-users to control the data flow [JKH20], the end-users may have limited influence on how their data is handled in the system. The following paragraphs will demonstrate concepts and list examples of technical developments that in various degrees aim to give end-users more control over data management.

Agent-based modeling or Agent-based Computing (ABC) is described as "computer simulations used to study the interactions between people, things, places, and time" [oPub16]. It can be used in the IoT ecosystem, which can then be referred to as a Multi Agent Systems (MAS), to model complex systems of components, their relationships, and interactions [SGP+20]. An agent represents an element capable of behavior and decision-making. Examples can be smart objects, devices or virtual entities [SGP+20], or even human users [Bon]. Neisse et al. [NBS+15] describe an agent-based framework for informed consent in the IoT, that uses pseudonyms for the control policies that regulate personal data. The framework utilizes the security toolkit SecKit [NBS+15; BBNT18], and claims to provide tools for informed consent among different categories of users and varying contexts, and give the user more control over the application's use of their personal data.

Moreover, Radio Frequency Identification (RFID) technology allows "things" to have a unique identity or tag, and be addressable within the IoT [HMM10]. Hancke et al. [HMM10] suggest that if users could have more control over RFIDs and associated data, they might actively contribute to the IoT by labeling objects and linking them to data entries or applications. This would require careful consideration of security and privacy within these tags. An example of a technical development that attempts to address this to increase the control of tags is Dimitriou's key-evolving RFID system [Dim16].

An example of a technical development regarding user privacy that can be labelled as more passive is the privacy preference model presented by Carminati et al. [CCFS16]. The model is claimed to give users more control over their data management within IoT platforms. It mandates users to specify their privacy preferences for which personal data attributes from their IoT devices that can be accessed, collected, used, and/or combined with other attributes to derive new information. In an example from [CCFS16], a user's step count, walked distance, heart rate and weight, gathered from their smart scale, step counter and fitness watch, can be combined to reveal the user's height, BMI, or other information about the user's physical state. Subsequently, the model supports using the stated privacy preferences for automatic generation of new privacy preferences to protect the new derived data [CCFS16], which is what can qualify as a passive mechanism. This is performed with the use of Complex event processing (CEP). CEP effectively analyzes data by combining information from different sources to look for patterns, and can respond in real-time [CFS+14]. It can be used in a distributed IoT architecture, which can be beneficial in terms of data management: the 'push' model allows for data to be provided to a system only when required, as not all data needs to be provided to the central system [RZL13].

Another technical development, specific to the smart home domain, is to have a decentralized architecture. In their IoT software architecture "Peekabo", Jin et al. [JKH20] aim to give the user more control over their data before it is sent to the cloud (and out of the user's control). Through the means of a user-controlled hub, repetitive data processing tasks are factored out from the cloud, and less personal data is sent over the network, which improves privacy [JKH20]. This reduction in data quantity helps reduce the risk of potential breaches or mishandling; when there are fewer data elements involved, there is a smaller chance of unauthorized dissemination or loss of control.

Finally, an example of building human control directly into the IoT system, is by using a human-in-the-loop model [NZS15].

2.1.3 User Interfaces and H2M Communication

The development of human-centric user interfaces and other means for human-to-machine (H2M) communication provides the user with a more active role in the IoT system. It allows for user engagement and customizing the technology to their needs [DAM17], and could therefore facilitate the involvement of the user in deciding how their autonomy should be carried out in the system. The subsequent paragraphs present emerging methods for H2M interaction such as the use of haptic interfaces, as well as other technical implementations that can enable the users to customize their service.

In the domain of driverless cars, haptic interfaces can be combined a human-in-the-loop approach for humans to take over when the intelligent system encounters unknown situations. Kuru et al. have developed a technical framework for this type of interaction [Kur21]. For the purpose of human supervision in fully autonomous self-driving vehicles, human-on-the-loop haptic teleoperation has been proposed as a means to allow human control in the event of challenging situations where the driver, i.e., an Artificial Intelligence (AI) agent, it not able to address the task at hand [Kur21]. This is done through the use of so-called digital twins, where an emulation of the real-world environment permits operation of the vehicle through haptic communication and feedback. Haptic technology concerns the use of force, vibration, or movement to stimulate the sense of touch, e.g., when a phone vibrates [Mas21]. So, the interface is in this case haptic and used for teleoperating a remote vehicle.

The Adaptive Remote Control System (ARCS) prototype is an example of another use case for human-centered interfaces. It is an IoT-based learning system which aims to improve differently-abled users' autonomy by giving access to and control over media devices such as TVs, tablets, and smartphones through a multi-level user interface [KZDB19]. As the user becomes more proficient in operating it, they can proceed to higher level requiring increased interaction.

Moreover, decision provenance is a method that intends to expose the decision pipeline in a system or a system-of-systems such as the IoT, to enable accountability [SCN19]. It is suggested that this leads to increased agency and empowerment among users, for instance helping them make better-informed decisions by making the consequences clear beforehand. However, more Human-Computer Interaction (HCI) research is required as to how the provenance data should be presented to different user groups in a meaningful way through interfaces, such as consumers, technical experts, regulators, auditors, etc.

Another technical development that requires a meaningful user interface is Baldini et al.'s Ethical Design framework [BBNT18]. As was described in the project proposal [Lei23], Baldini et al. have introduced the concept of Ethical design, which seeks to empower users in their interaction with the IoT. They proposed a policy-based framework called SecKit, which grants users greater control over their personal data and IoT services by enabling them to select sets of policies. The framework operates by regulating the usage of IoT devices through profiles that contain rules specifying conditions for activating enforcement policies. However, the effectiveness of the framework relies on the availability of user interfaces that facilitate the generation, modification, and customization of these profiles in a seamless and efficient manner.

Finally, in a smart home context, IoT devices can be vulnerable to unintended user access within the home [JCP17]. Jang et al. [JCP17] advocate for more fine-grained access control and authentication by allowing for configuration of different user profiles with varying access privileges. However, they do not provide an explanation to how the user should interact with the system to configure this kind of access control.

2.2 Regulatory Frameworks and Legal Considerations

In this section, a selection of aspects pertaining to legal frameworks surrounding the IoT is presented. This holds significance due to the rapid advancement of the technology, which is outpacing the ability of standards and legal bodies to adequately respond. Legal frameworks play a crucial role in safeguarding users and governing the activities of IoT manufacturers and the broader IoT market [Kar21]. It should be noted that this section does not provide an exhaustive survey of all existing IoT laws. Rather, it aims to underscore select current legislation and important challenges that lie ahead. Firstly, a brief overview of general legal considerations in the IoT globally is given, followed by two examples of more specific use cases.

The main law that exists in Europe pertaining data protection and privacy is the European Union General Data Protection Regulation (GDPR), which imposes obligations on entities regarding data collection, processing, storage, and protection for personal data [Uğu23; Kar21]. This regulation is applicable to IoT ecosystems, as IoT devices collect and process vast amounts of personal information. Most of the legal aspects in Europe are concerned with cybersecurity. EU's Cybersecurity Act of 2019 strengthens the capacity of the European Union Agency for Network and Information Security (ENISA) to address cybersecurity risks and vulnerabilities of IoT devices [Kar21]. Additionally, the ETSI TS 103 645 Standard, based on the UK's Code of Practice for Consumer IoT Security, focuses on the cybersecurity of user-related IoT devices and provides provisions to regulate and enhance users' digital security and privacy [Kar21].

Yet to be implemented is EU's ePrivacy Regulation (ePR). The ePR focuses on data privacy in electronic communications and covers IoT among other areas to ensure secure communication of information within networks and devices [Kar21]. Lastly, the UK Government has launched proposals and codes of practice targeting consumer IoT security. These proposals emphasize strong cybersecurity measures in IoT devices, including unique and strong passwords, contact information for reporting vulnerabilities, and clear mention of potential security updates at the time of purchase.

In the United States, the Internet of Things Cybersecurity Improvement Act 2020 sets minimum cybersecurity standards for IoT devices owned and controlled by the federal government [Uğu23]. Additionally, California's IoT Cybersecurity Act SB-327 mandates manufacturers of IoT devices to include reasonable security measures to protect the devices and data [Uğu23].

In the rest of the world, different laws and standards have been implemented or proposed, in the following countries/regions: India, China, Japan, United Arab Emirates (UAE), Australia, Brazil, Argenina, and Chile. Karale [Kar21] gives an extensive overview of these.

Moreover, there exist laws and standards wherein several nations have enacted together internationally, namely the **Statement of Intent Regarding the Security of the Internet of Things** between Australia, Canada, New Zealand, UK, and USA, as well as International Standard or ISO standards to address various aspects such as interoperability, architecture, application programming interfaces (APIs), data exchange, edge computing, and IoT security and privacy [Kar21].

In conclusion, while existing regulations in various countries address some aspects of IoT technology, there is a need for comprehensive and consistent legal frameworks that consider data protection, privacy, cybersecurity, liability, and potential human rights infringements [Uğu23; Kar21]. On top of that, these laws and standards fail to address how to secure IoT from an ethical standpoint, and how consumers are to be made aware of the operation of these systems [Kar21; Uğu23].

Specific Use Cases

In [FS15], Fernandes and Sivaraman have examined the implications of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* that was passed in Australia in 2015, deeming it in need of amendment to restrict the possibility of non-stop, involuntary and ubiquitous monitoring of individuals.

In [GVK19], Garg et al. discuss legal issues specific to fog and cloud environments. They suggest that the scope and complexity of managed systems (IoT-Fog-Cloud environments) can weaken user control over private data, and that the responsibility of data protection is shifting towards service providers.

2.3 The Human-centered Perspective

The following section will explain concepts and terms related to the human-centered aspects of this thesis, and to how the term human autonomy is defined and understood. This includes several interpretations of autonomy from the literature, as well as a selection of features that are goals of human-empowering IoT design, namely agency, empowerment, and control [YAP+23]. Lastly, a brief explanation of Self-Determination Theory (SDT) theory is featured. SDT posits that autonomy is one of three fundamental needs for humans to function optimally.

2.3.1 Definitions of Autonomy

Human autonomy is a complex and intricate concept, and there are a number of different definitions of the term. This makes it difficult to address the risks technology poses to autonomy, seeing as the threats can differ depending on which definition of autonomy has been used [Dai17]. The research in this thesis focuses on three definitions, namely, personal, moral, and political autonomy, as described by Dainow in [Dai17]. However, other approaches to understanding the term will be briefly explained in the subsequent paragraphs.

In his work titled "Threats to Autonomy from Emerging ICTs", Dainow introduces the conceptualization of moral autonomy in Western Philosophy as "the capacity to determine one's own moral codes", and further extends this notion to include the concepts of personal and political autonomy [Dai17]. As per Dainow's analysis, these three facets of autonomy share a common thread: self-determination. Table 2.1 provides an explanation of moral, personal, and political autonomy.

Table 2.1: Definitions of human autonomy [Dai17].

Definition	Literature statement
Moral	The capacity of individuals to determine their own moral codes and make moral judgments independent of external authority. Moral autonomy is about the ability to decide what is right or wrong based on personal principles and not simply following rules.
Personal	The capacity of individuals to determine their own actions and make choices that align with their own desires and preferences. Personal autonomy emphasizes self-governance and the freedom to act according to one's own will.
Political	The capacity of individuals to make their own political decisions and have those decisions respected by others. Political autonomy focuses on the ability to participate in the political process and shape the governance of society.

Laitinen and Sahlgren [LS21], on the other hand, suggest that to achieve full degree of autonomy, six key elements must be fulfilled. The multi-dimensional model requires the following aspects to be realized jointly for this purpose [LS21]:

1. Potential and developed capacities for self-determination.
2. The normative requirements or duties of others (and oneself) to respect and support one's autonomy.
3. The recognition or respect by others, as a response to such requirements, and the relational autonomy this constitutes.
4. Self-respect and other forms of positive self-relation.
5. The performative aspect of realization or actual exercise of the capacities.
6. Various material, economic, legal, cultural, and informational resources can be understood as comprising necessary preconditions for autonomy in these dimensions.

Furthermore, in their work "AI Systems and Respect for Human Autonomy", Laitinen and Sahlgren [LS21] distinguish human autonomy from functional autonomy, which refers to a system's ability to operate independently. Human autonomy, in contrast, encompasses self-determination and self-rule, going beyond mere functional independence. It also incorporates a certain level of control over instincts and impulses, which is lacking in most animals. This control is according to Laitinen and Sahlgren essential for the concept of moral responsibility. It is closely linked to practical rationality, which refers to the capacity to assess reasons for action and pursue valuable goals. This capacity allows humans to make reasoned decisions and resist irrational impulses. Moreover, the text clarifies that the focus is on personal autonomy rather than collective, moral, or political autonomy. It also differentiates between a sense of autonomy and personal autonomy itself. While the focus is on philosophy and theory, the text acknowledges that the proposed model could be used as a basis for future empirical research, including studying people's experiences of autonomy.

Another approach to understanding autonomy is the one made by philosopher Gerald Dworkin, who is a professor in moral, political and legal philosophy, and specializes in research on the nature and justification of autonomy among other subjects. In his book "The Theory and Practice of Autonomy", Dworkin sums up the notion of autonomy in the following way [Dwo88]:

> *Putting the various pieces together, autonomy is conceived of as a second-order capacity of persons to reflect critically upon their first-order preferences, desires, wishes and so forth and the capacity to accept or attempt to change these in light of higher-order preferences and values.*

According to Dworkin, autonomy is not just about following immediate desires, but involves the ability to step back, think critically about those desires, and make choices based on a deeper understanding of personal values and long-term goals. In the book, Dworkin also discusses implications of autonomy in relation to proxy consent, informed consent, and paternalism.

Agency, Empowerment, and Control

As noted above, agency, empowerment, and control are important goals of human-centric IoT design [YAP+23]. These concepts can also be viewed in relation to autonomy. According to the Stanford Encyclopedia of Philosophy, agency is the power to decide and act, while autonomy is about having control over those choices and actions [BW18]. This means that agency can be seen as a prerequisite for autonomy; without the ability to act and make choices, an individual would lack the capacity to exercise autonomy. Moreover, empowerment can be defined as a multi-dimensional social process aimed at providing people with the capacity to control their own lives, and acting on issues they deem important both in their lives, but also in their communities and society [PC99]. Since empowerment entails the capacity to exert control, it can be seen as enabling of autonomy. Lastly, each of these concepts entails an element of control, underlining its important role in autonomy.

Self-determination

The element that all understandings of human autonomy seem to have in common, is self-determination [Dai17; LS21]. Self-Determination Theory expresses autonomy as a requirement for humans' optimal growth and positive development [ALR17]. SDT is a macro-theory, meaning that it concerns society and humanity instead of pertaining to the individual. It studies human motivation, and describes the particulars of human agentic action [ALR17]. SDT states that the three basic psychological needs humans have to fulfil to be self-determined are competence, relatedness, and autonomy [ALR17]. Moreover, SDT posits that autonomy is one of the most important components for human well-being [ALR17; LS21].

2.4 Human Autonomy in the Technical Context

Historically, the motivation behind creating new technology has often been driven by the desire to push the boundaries of what is possible technologically [BP06]. This means that scientists, engineers, and inventors have been motivated by the challenge of innovation and have sought to discover and develop new technological solutions, often without putting the immediate emphasis on addressing human needs. While technology advancement can undoubtedly lead to numerous benefits and improvements in various aspects of life, it is essential to ensure that it aligns with the needs and values of humanity, rather than just being developed for the sake of novelty. A truly human-centric approach to technology development involves understanding and addressing real-world problems, human experiences, and ethical considerations to create meaningful and relevant technological solutions [BP06]. The question remains how to translate principles of human autonomy to be implemented technically into IoT systems [YAP+23], especially when implementing ethical processing can lead to imposing someone's particular values on the system without knowing whether said values align with the users' values [Dai17].

In the coming paragraphs, a selection of examples will be presented where the developers have used human-centric approaches, principles, techniques, theories, or legal frameworks, to build IoT systems or mechanisms that configure in human autonomy.

In their work "Motivating Users to Manage Privacy Concerns in Cyber-Physical Settings — A Design Science Approach Considering Self-Determination Theory", Oppl and Stary have addressed the three dimensions of SDT, i.e., autonomy, competence, and relatedness, to derive four design requirements for user-centric privacy management in the IoT that enable a more active user involvement [OS22]. The requirements are (1) transparency of data collection and processing, (2) privacy preference specification, (3) available context information, and (4) privacy options setting and monitoring og system behavior [OS22]. The article also explains how each requirement fulfills the three SDT dimensions.

Another development that resulted in a set of design requirements, was the SONOPA (SOcial Networks for Older adults to Promote an Active life) study from 2016 [AJD+16]. The research set out to develop and test an Ambient Assisted Living (AAL) solution based on sensor technology, that aimed to empower elders to stay active and autonomous. Social scientists as well as engineers were involved from the beginning to establish a multidisciplinary approach [AJD+16]. A user-centered method was utilized to investigate the needs, wishes, and requirements of potential user groups by acquiring insights from older adults and their caregivers in all stages of development. In the end, a set of eight non-technical design requirements that can guide future development of AAL technology were produced, as described in [AJD+16].

A different study that also resulted in a set of design principles for AAL technologies, was the narrative literature review study "New Ambient Assisted Living Technology: A Narrative Review" by Constantinou et al. from 2021 [CGM+21]. By looking at reasons why older adults accept new technology, the N-ACT principles (Needs, Adjustability, Control, Trust) were developed to help design AAL technology that will actually be used by the end-users [CGM+21]. Important for the N-ACT principles is the Control principle, which states that technology should be a tool for serving human needs and not the other way around.

Lastly, an example of using a legal framework to try to build accountability into the IoT is Crabtree et al.'s IoT Databox model [CLC+18]. GDPR is the legal framework that mandates accountability in digital technology, in which Crabtree et al. focus on what is called "external" accountability. This involves revealing the hidden activities and connections of interconnected devices and the social contexts they operate within [CLC+18]. The model is aimed at enabling consent, transparent data processing, fine-grained data flow management, online access, and data portability, through different components described in [CLC+18]. Though, what still lacks is to verify whether the IoT Databox model meets human needs thrugh industry and end-user perspectives.

2.4.1 Research Gap

In a broad sense, there is a lack of research focusing on what is needed to secure the IoT from an ethical viewpoint [Kar21]. As seen from the examples in this chapter, a lot of attention is gradually being directed towards privacy and security in the

IoT realm, both through legal frameworks and developments in communication and information security. Yet, the IoT presents an ethical threat to common users, often without their awareness, potentially resulting in unfavorable situations for them [Kar21]. Moreover, less attention is given to larger ways in which IoT technology is used. These bigger operational situations involve various technical parts that might be controlled by different groups or organizations, who work together to make specific functions happen [SCN19].

More specifically, since human autonomy can be said to essential for well-being [ALR17], it is of interest to preserve it in future intelligent environments. As stated previously, the question still remains how to best translate the requirements of human autonomy to be technically implemented in the IoT [YAP+23]. Existing developments have focused on design frameworks, architecture, user interfaces, and user monitoring, but few have been developed with the involvement of end-users from the beginning [YAP+23]. However, it is possible to involve end-users in this translation process as well [YAP+23]. One step towards agreeing on a technical translation of autonomy can be to investigate and compare interpretations of autonomy among experts and the public view to see what they place emphasis on, as well as look into their perspectives on factors that can enable or hinder autonomy in the IoT.

2.5 Related Works

The topic of how technology influences autonomy has been researched in various contexts. This section will introduce related research where the authors have explored autonomy or other ethical aspects in relation to the IoT or other technology, works that involve mapping barriers and enablers of ethical technology development, and studies that aim to say something about the future of human autonomy in the context of IoT.

Ambient Intelligence or ubiquitous computing is a concept that has been described numerous times by IoT enthusiasts, researchers, and visionaries. According to Burgleman and Punie [BP06], Ambient Intelligence (AmI) constitutes the vision of a future society where technology is seamlessly built into the environment, preferably invisible, and allows for communication among the people, devices, and environment in real-time. Everything should be connected and always available, adapting to different contexts and humans' preferences. A human-centric approach to AmI is expressed, where the basis is the needs of users and not where and how new technical solutions can be applied. Punie [Pun05] also describes H2M interactions becoming more similar to human-to-human interactions, bringing senses like touch as well as gestures and speech into play.

Burgleman and Punie's "Information, Society and Technology" discusses the

2001 report by Information Society Technologies Advisory Group (ISTAG) where four future AmI scenarios were developed, along with foresight studies and Delphi exercises performed to research the emerging information society in European [BP06]. The article renders 15 key social drivers for future information technology identified by the Foresight on IST in the European Research Area (FISTERA) network [BP06]. Information Society and Technology (IST) is a priority of the sixth Research and Technological Development (RTD) Framework Programme (FP6) of the European Union (EU) [BP06]. It is stated that the IST community aims address societal, social, and economic challenges in Europe through the use of AmI. Punie also discusses the future of AmI in Europe, where he advocates that in addition to having humans in the center, AmI would benefit from including an everyday-life perspective in its vision [Pun05].

A large and somewhat more recent study is the ETICA project on ethical issues in emerging information and communications technology (ICT) technologies[1]. ETICA was a foresight study involving various stakeholders and multidisciplinary perspectives, resulting in guidelines on how to effectively address ethical aspects of emerging ICT. The project identified 107 different emerging technologies that were aggregated into eleven groups, where Ambient Intelligence was one of the groups [Dai17]. Around 400 ethical concerns were identified in relation to these groups.

Dainow applies the ETICA project and the identified technology groups in his discussion of how emerging ICTs threaten human autonomy [Dai17]. Among the discussed technologies is AmI. He also considers how a range of different definitions and interpretations of the term autonomy can be problematic for ethical technology design, and advocates for a more flexible approach where ICT should be developed to be adaptable to the user's values.

A more recent study with a future perspective is Sineviciene et al.'s research on the socio-economic and cultural effects of disruptive technologies, among them IoT and IoT-related developments [SHK+21]. The authors have analyzed the characteristics of Industry 4.0 to list the disruptive technologies and their associated socio-economic effects. The effects are categorized as either positive or negative, whereupon an explanation is given to how and why the effects are relevant to the different technologies.

Another study with a future perspective, that also describes drivers and challenges for ethical design and deployment of the IoT is Baldini et al.'s framework "Ethical Design in the Internet of Things", which is elaborated in [BBNT18]. The article lists eleven ethical IoT challenges as well as a set of four processes that express drivers and challenges to the ethical design framework they provide.

[1] https://www.etica-project.eu

Similar approaches, i.e., categorizing factors as drivers and impediments or enablers and inhibitors, have been used by Spiekermann et al. to examine drivers and impediments of ethical system development [SKL18], and in larger scale by the European Network and Information Security (NIS) Platform to establish a cybersecurity strategic research agenda (SRA), expressing enablers and inhibitors of individuals' digital rights, a resilient digital civilisation, and a trustworthy infrastructure [BMG15]. However, the methodologies differ between the two. Spiekermann et al.'s research is based on a survey of 124 engineers and interviews with 6 senior engineers, whereas the SRA was created through expert meetings and brainstorming sessions. Nevertheless, both studies resulted in categorization of enablers and barriers. The SRA, in particular, displays more extensive and systematic categorization, as can be seen in [BMG15].

A study that actively addresses human autonomy is Laitinen and Salhgren's "AI Systems and Respect for Human Autonomy", in which the authors have mapped various ways AI systems can promote human autonomy or hinder it [LS21]. To explore this, the method employed philosophical reflection guided by literature on ethics and human autonomy [LS21]. The article begins with stating six aspects that need to be fulfilled to achieve full autonomy, followed by a description of different ways AI can support of inhibit it [LS21].

Lastly, Pew Research Center have canvassed the opinions of 540 multidisciplinary experts about how much control humans will have over decision-making as the use of AI and digital systems grows, in their extensive report "The Future of Human Agency" [23]. For this purpose, they developed two distinct scenarios: one which assumes technology will be designed to allow humans to easily be in control, and one which assumes technology will not be designed in this way[23]. The participants were asked to imply which scenario they believe will happen, and provide reasoning to their answers. However, it is worth noting that the so-called "canvassing" is nonscientific, and therefore caution is required when interpreting the results.

The manner in which the research in this thesis differs from the abovementioned studies is by aiming to compare perspectives of experts with those of the public view. The work focuses on different interpretations of human autonomy and what they imply for technical IoT translations of the term, as well as seeking to identify the most important barriers and enablers that need to be addressed to ensure human autonomy in future IoT. Having set the context, the next step is to closely examine the methodology used in this thesis. In the upcoming chapter, the approaches used to address the Research Questions specified in Section 1.2 will be explained and justified.

Chapter 3
Methodology

This chapter describes and justifies the methodology used in the different parts of the data gathering for the thesis. The selected methodology aims to investigate interpretations of autonomy, as well as map the current main barriers and enablers of human autonomy in the IoT, and assess their importance for future use and design of IoT according to expert opinions and the public view, using qualitative and quantitative methods.

3.1 Research Design

As a novice researcher in the field of human autonomy in IoT, it was necessary to deepen the understanding of the topic, and explore literature. The research design first involved a mapping of the technical solutions that are in use for enabling or protecting human autonomy, or the present obstacles or barriers to preserving human autonomy in the IoT. Then, in order to identify the importance of the associated enablers, and barriers the understanding of autonomy, and degree of importance of the factors were investigated in two quantitative studies, one targeting experts and the other end-users. See Figure 3.1 for an overview of the complete methodology.

The first research phase, a systematic literature review, aimed to identify existing technical solutions in multi-disciplinary academic sources that address how to incorporate human autonomy technically in IoT. In addition, it was important to investigate whether anyone else had attempted to map the main inhibiting and enabling factors that influence the level of human autonomy in the IoT. A systematic literature review was chosen as the preferred methodology for addressing Research Question 2 (see Section 1.2). By providing a comprehensive mapping of existing evidence, a systematic literature review facilitates the identification of areas that require further research as well as the discernment of questions for which the literature already offers conclusive insights [Els]. Thus, this methodology was deemed appropriate for achieving the aforementioned research questions.

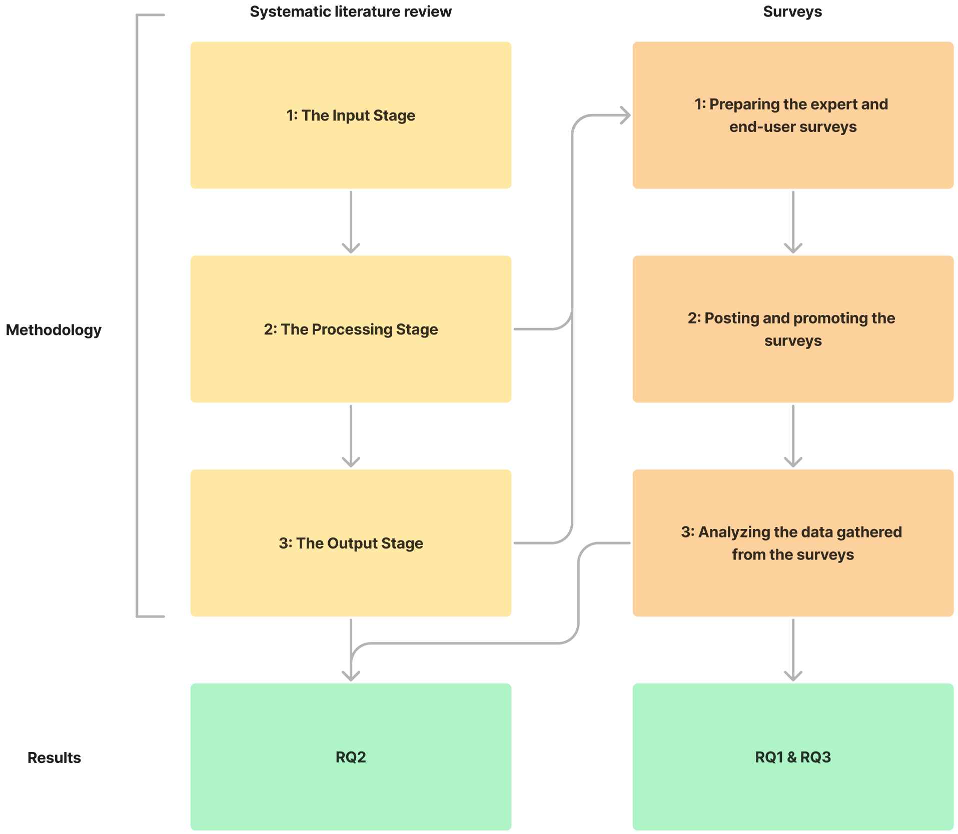

Systematic literature review
Surveys
Methodology
1: The Input Stage
2: The Processing Stage
3: The Output Stage
1: Preparing the expert and end-user surveys
2: Posting and promoting the surveys
3: Analyzing the data gathered from the surveys
Results
RQ2
RQ1 & RQ3

Figure 3.1: An overview of the complete methodology and how the different parts of it produced the results.

The second research phase was the evaluation of factors derived from the systematic literature review, with the aim of addressing Research Questions 1, 2, and 3 specified in Section 1.2. To accomplish this, two surveys were developed: one targeting domain experts and the other targeting the general public. The primary goal of these surveys was to validate the findings from the literature review and to establish the degree of agreement or divergence between expert opinions and public perspectives regarding the definition of 'human autonomy', as well as the identified factors' importance in future design and use of IoT devices. Given the complexity of the topic, the initial intention was to exclusively survey experts who possess domain-specific knowledge. Expert opinions are valuable, particularly in forecasting tasks where limited information is available for statistical analysis [RW01]. However, since consumers ultimately are the end-users of IoT devices, they hold substantial importance as stakeholders. Moreover, there is a lack of scientific research into incorporating diverse and multi-stakeholder perspectives into the technical development of human-centric IoT [YD23], including end-user requirements for retaining their agency in the system. Hence, their perspectives were considered valuable and warranted inclusion in the surveys.

Ultimately, the choice of methodology was a combination of a systematic literature review and surveys of both experts and consumers. As mentioned above, Figure 3.1 gives an overview of the full methodology, and depicts how its different parts produced the results to the research questions.

3.2 Systematic Literature Review

A literature review is traditionally performed to prepare a conceptual foundation and build theory for hypotheses formulation in a thesis, as well as to identify research gaps in previous research on the subject in question. It can be presented as background and related works to the thesis research, such as Chapter 2 of this report. However, to incorporate a literature review as part of the methodology, it is essential to undertake appropriate measures to ensure its accuracy, precision, and trustworthiness, as suggested by Snyder [Sny19]. As part of this project, a systematic literature review was conducted, more specifically a qualitative systematic review [Sny19]. This review follows a strict process for article collection to ensure replicability, and employs a predominantly qualitative content analysis approach to analyse and evaluate the articles.

The systematic literature review serves several purposes. Primarily, it serves as a basis for providing answers to Research Question 1 introduced in Chapter 1. Secondly, in order to build a solid theoretical foundation for the thesis and to clarify in which parts of already-existing research to contribute, an overview of what has been done so far is needed. Thus the literature from the review, along with the literature identified in the project proposal [Lei23] for the thesis, is used in Chapter 2 to present the background context and related works of existing technical solutions and concepts. Lastly, the literature review should facilitate and provide justifications for the selection of methodology for the rest of the thesis [LE06], namely the surveys presented later in this chapter.

The literature review follows a systematic approach, with key elements from Levy and Ellis' framework on conducting an effective literature review for Information

Systems research [LE06]. The framework describes three stages in a literature review. The first stage or the input stage, is to find and collect literature. Second is the processing stage, where the literature is screened and filtered to be included or excluded in the review based on specified relevance criteria. Lastly, the output stage is performing analyses, documenting and writing the review itself. The results of the literature review are presented in Chapter 4.

The goal of the systematic literature review has been to examine relevant articles to identify the current main factors that can enable and inhibit autonomy in IoT, and to explore whether similar research has been conducted recently.

3.2.1 The Input Stage

In the beginning of the input stage, a search strategy was developed in an attempt to seek out multi-disciplinary scientific research targeting the design outcomes of human autonomy, empowerment, agency, and control, and the existing technical configurations and factors. It was important that the search strategy be as relevant as possible, therefore no limitations were set in terms of geographical location or time of publication. Keyword search was employed as the method for finding literature, so the first step was to identify the keywords and search terms in existing theory, to be used in the search. Along with the research questions, the keywords identified in the project proposal [Lei23] were used as a starting point for test searches, and after scanning the appearing literature more relevant keywords, such as separating between human and user, were iteratively tested. The iterative process produced three categories of keywords that were combined into one search string, as shown in Figure 3.2. The first category considers human-centered design outcomes related to human autonomy, as explained in Chapter 2. Both the words 'human' and 'user' were used in front of each of the keywords in this category. The second category contains different technology definitions of the IoT. Lastly, the third category consists of synonyms for factors, i.e., aspects that can influence human autonomy in the IoT, either by enabling, inhibiting, or affecting it in some other way.

Breadth in the literature search is important for the quality of the review [LE06], hence the same keyword search was performed in several academic databases. The databases used were Web of Science[1], Scopus[2], IEEE Xplore[3] and ACM Digital Library[4]. The scope of these databases includes literature on ICT as well as multidisciplinary literature. Appendix A displays the full search syntax used in the different databases, how many hits each search yielded, and the dates of when each of the searches were performed.

[1] https://www.webofscience.com

[2] https://www.scopus.com

[3] https://ieeexplore.ieee.org

[4] https://dl.acm.org

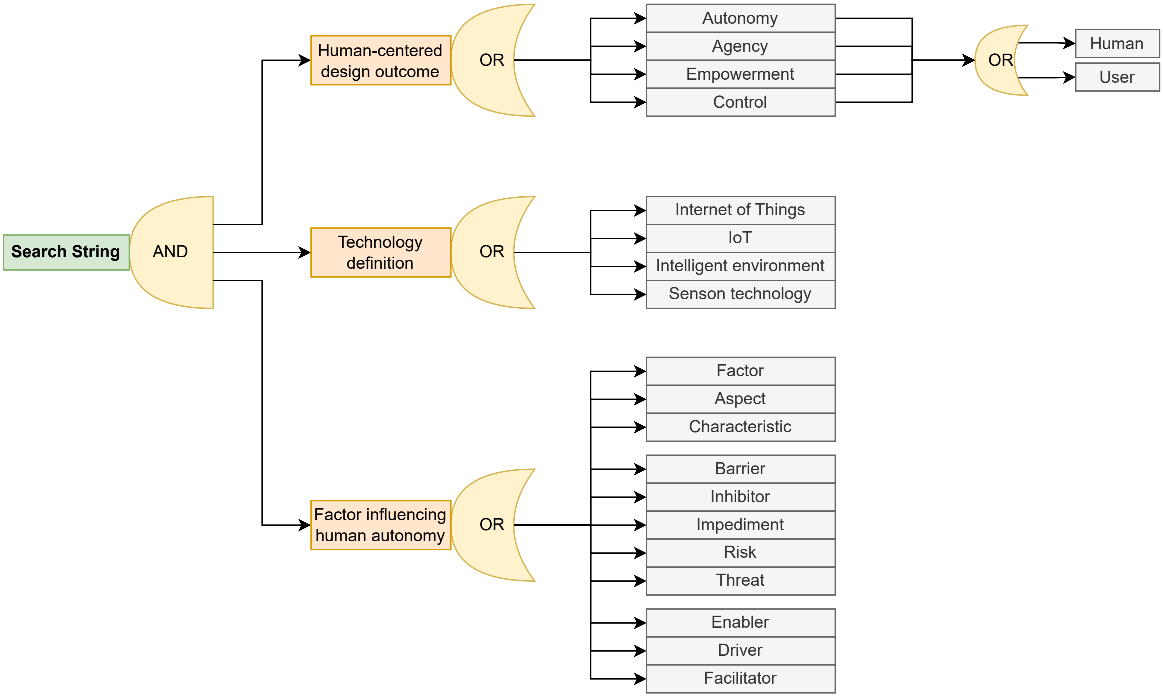


Figure 3.2: Logic diagram of the search string used for the keyword search.

3.2.2 The Processing Stage

A comprehensive selection protocol was devised in advance to establish objectivity and relevance. The protocol was designed with the research questions in mind to ensure that the review incorporates literature of adequate quality, relevance, and applicability. Specific criteria were established for the inclusion and exclusion of articles, which can be viewed in its entirety in Appendix B for further details. According to the protocol, literature was included if it discussed aspects pertaining to human autonomy in the context of the IoT, such as mechanisms that either preserve or enhance, or diminish or impede human autonomy, agency, empowerment, or control. Additionally, literature discussing the definition of human autonomy and/or its technical and non-technical requirements within IoT context was considered for inclusion. Literature was excluded if it only superficially referenced human autonomy or the aforementioned related terms, or if the work was solely oriented towards business or technology. The review encompasses various types of works, including research and journal articles, conference proceedings, workshop papers, and book chapters.

The database searches were performed on March 1st, 6th, and 15th, 2023, specifically targeting the Title, Abstract, and Keyword fields of the literature. The initial keyword search yielded a total of 84 articles, which was subsequently reduced to 62 after eliminating duplicate entries. A detailed screening process based on the selection criteria, comprising of the examination of titles, abstracts, and keywords, further narrowed down the selection to 46 articles. After a thorough assessment of the full texts, five articles were excluded that failed to meet the criteria. These exclusions were based on the articles' predominant orientation towards business or technology, as well as demo papers lacking substantial contributions. As a result, the final count stood at 41 articles. A visual representation of this selection process can be found in Figure 3.3.

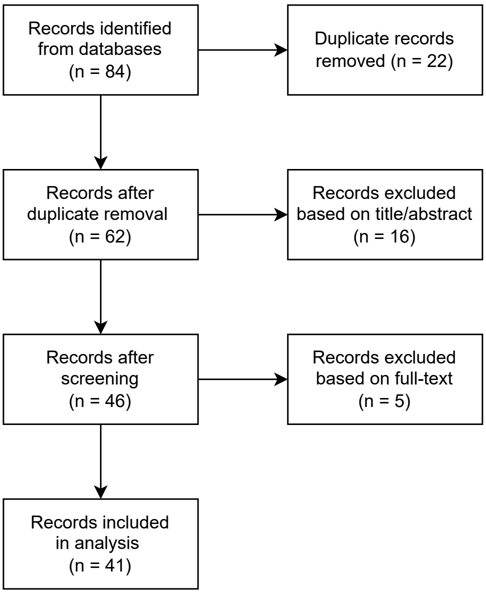

Records identified from databases (n = 84)
Duplicate records removed (n = 22)
Records after duplicate removal (n = 62)
Records excluded based on title/abstract (n = 16)
Records after screening (n = 46)
Records excluded based on full-text (n = 5)
Records included in analysis (n = 41)

Figure 3.3: Flow chart of the literature selection process.

To conduct a critical appraisal of the selected articles, the CRAP test [BG20] was employed as a guiding framework. The CRAP test evaluates four key dimensions of a piece of literature, namely currency, reliability and relevance, authority, and purpose and point of view. The currency criterion takes into account the publication date, ensuring the information is recent and pertinent to the topic at hand. The reliability and relevance principle examines the information's source, availability of methodology and references for verification, peer-review status, and whether it adopts a single- or multidisciplinary perspective. Authority focuses on the credentials of the authors and the associated organization or company. Finally, the purpose and point of view dimension considers the authors' intent, target audience, and the article's overarching purpose (e.g., informative, persuasive, commercial, or entertainment-oriented).

3.2.3 The Output Stage

The aim of this stage was to gain overview of existing knowledge on factors influencing human autonomy in the IoT. To extract the essence from each piece of literature, a qualitative content analysis was conducted. More concretely, an Excel coding scheme was utilized for categorization of common themes. Some of the factors were highly specific, so to understand the overarching themes in the literature, an attempt was made to organize them into high-level factors. The different high-level factors became apparent during the analysis of the literature and the sorting of the specific and lower-level factors into the Excel coding scheme. Each article was coded according to the variables/themes and corresponding categories summarized in Table 3.1.

Table 3.1: Themes each article was sorted according to in the Excel coding scheme.

Theme	**Explanation**
Title	Title of the piece of literature.
Author	Author(s) of the piece of literature.
Geography	Location of associated university or place of research.
Perspective	**Point of view: multidisciplinary or single discipline.**
Expertise	Field of research of the author(s).
Design outcome	**Human-centered design outcome (i.e., autonomy, agency, empowerment, control, security, privacy, and trust).**
Framework	**Design framework (Design principles guiding the development of technical IoT solutions**)
Factor	**Aspect influencing human autonomy in IoT in some way.**
High-level factor	**High-level factor that encompasses several lower-level factors.**
Future research	Identified topics requiring more research and research gaps.
Technical solution	Specified technical solution to achieve human-centered outcomes in IoT.
Theory	Theories for design, or other theories discussed in the piece of literature.

The themes that were most important for the analyses are outlined in bold. The coding process of the thematic analysis was done manually after reading and interpreting each article. In addition, the statistical software program SPSS[5] was

[5] https://www.ibm.com/products/spss-statistics

used to perform simple statistical analyses of the general characteristics of the articles, as well as which theories and frameworks they applied. The results of the systematic literature review are presented in Chapter 4, Section 4.1.

According to Oxford Languages, a factor can be defined as "a circumstance, fact, or influence that contributes to a result or outcome" [Dic02]. To clarify, in this research, a factor is considered as anything that affects human autonomy, specifically described in the literature to have an impact on autonomy or any of the three related human-centered outcomes: agency, empowerment, and control. An enabler is defined as any technical or non-technical factor that promotes or preserves autonomy and/or the outcomes, and a barrier is defined as any factor that hinders or undermines autonomy and/or the outcomes.

3.2.4 Limitations of the Literature Review

Levy and Elis have identified two main limitations that may occur during the course of a systematic literature review, namely narrowness and shallow depth of the literature background [LE06]. Narrowness in the literature background can occur when conducting a keyword search using only one or two databases [LE06]. To address this potential limitation, this review employed queries across four distinct databases, broadening the scope of the search. Furthermore, the utilization of technology-specific terms or trendy Information technology (IT) buzzwords can lead to a shallow depth of literature background, as these buzzwords tend to fluctuate in their prevalence within literature over time [LE06]. To counteract this limitation, the search process underwent several iterative phases, incorporating newly identified keywords as they emerged within the literature. This approach enhanced the robustness of the search methodology and mitigated the impact of said limitation.

Although employing a systematic approach to literature selection helps mitigate the introduction of systematic error [Sny19], this review is sill susceptible to certain types of bias. Biases may have occurred during the article collection phase due to lack of limited expertise in the field of research. However, the involvement of experienced supervisors in devising the selection criteria has aided in minimizing this risk. The analysis of articles, conducted manually and qualitatively, introduces the potential for information bias. It is possible that certain aspects were overlooked, missed, or incorrectly classified. Nevertheless, a comprehensive Excel categorization scheme was designed in collaboration with the supervisors to capture relevant information and minimize bias. Furthermore, Section 3.2 provides a detailed account of the literature review procedure, enhancing transparency, reproducibility, and subsequently reducing potential bias.

3.3 Surveys

The second part of the methodology aims to understand different interpretations of the term human autonomy, to verify the findings from the systematic literature review, and to determine the importance of the identified enablers and barriers for future IoT. To do this, two surveys were utilized, one targeting experts and one end-users. Throughout this report, the two surveys will be referred to as the expert survey and the end-user survey, and the participants as the experts and end-users, users or consumers.

The following subsections will explain how the surveys were designed to include elements from Foresight and the Delphi exercise, and how different approaches were utilized to query experts and end-users. Moreover, the questionnaire designs are described, as well as the survey implementation and related operational aspects, as well as methods for data analysis. Lastly, an overview of the survey limitations is given.

3.3.1 Survey Design

To research how the subject of human autonomy in the IoT is perceived among various stakeholders, the decision was made to perform two different surveys for experts and end-users. The surveys contained inquiries about the participants' definition of human autonomy, their level of agreement to whether the factors from the literature review truly are enablers and barriers, and how significant they are perceived to be in contributing to a positive and a negative scenario about future IoT. The surveys were designed to utilize both qualitative and quantitative strategies to gather data, i.e., open- and close-ended questions, respectively.

Elements from Foresight and the Delphi Method

The two main purposes of the surveys were to investigate the understanding of human autonomy, and to evaluate the factors identified in the literature review in an attempt to ascertain their significance as barriers and enablers of human autonomy in future IoT. When attempting to consider the future in a methodical manner, one proceeds into the realm of 'Foresight studies' [Dai17]. The Delphi method is an approach within the foresight discipline, which seeks judgement from experts on a topic. It was introduced quite thoroughly in the project proposal [Lei23], but a recap from Miles et al.'s description of the Delphi method in their book Foresight for Science, Technology and Innovation (ForSTI) is provided below [MSS16]:

The Delphi method facilitates gaining consensus among experts and stakeholders from different disciplines. The method entails administrating anonymous surveys to capture expert knowledge and can be particularly useful in investigating topics characterized by substantial uncertainty about the future and future situations [MSS16]. Distinct from conventional survey methodologies, the Delphi method is designed to be iterative, enabling participants to receive feedback on their initial responses and revise their answers in light of information obtained from other respondents. This feature facilitates insightful analysis, an makes the Delphi a valuable tool for investigating whether there is consensus or not among different perspectives [MSS16].

Several advantages are associated with the Delphi method, which may also apply to the expert survey in this thesis. According to Skinner et al.'s review of the Delphi method as a research strategy in information systems, by keeping participants anonymous, one is decreasing the chances of a "follow-the-leader" tendency in a group of experts [SNCL15]. Anonymity also avoids direct confrontation between the participants, encouraging honesty and thwarting group pressure [SNCL15]. Though, Delphi surveys have some drawbacks as well. It is especially time consuming, and it can be difficult to recruit participants. Additionally, dropout rates can be high since the execution requires several iterations.

A Delphi survey was originally considered as the methodology for the second part of this study, but due to both time and resource constraints, a decision was made to conduct regular online surveys instead, with only one iteration. Additionally, the choice was made to survey the general public as well as experts, in case there would be too low a response rate among the experts. Nevertheless, since the objective was to study the future, some elements from the Delphi technique were implemented in both surveys. As recommended by Gallego and Bueno [GB14] in their exploration of the application of Delphi in information systems and technology research, both open- and closed-ended questions were included in the surveys. Open-ended questions are what facilitate gaining consensus, and closed-ended questions allow the participants to express their perception of the importance (or lack thereof) of the given factors [GB14].

The exploration of future scenarios is also a ForSTI element. In a Delphi survey, the experts can be asked to stipulate measures that need to be implemented in order for a scenario to be fulfilled within a certain time frame [MSS16]. In these surveys, the measures (i.e., factors) were already provided, and participants were ask to rate their importance for realizing the given scenarios. In addition, they were given the opportunity to specify other relevant factors at the end of the survey. The use of a Likert scale is also recommended [GB14; SNCL15]. A choice was made to implement a Likert scale with seven points instead of five, due to the fact that there would be only one iteration of the surveys, and it was desirable to extract more detailed and nuanced responses. The expert survey contained another typical Delphi element, namely the rating of desirability and likelihood of the given scenarios [MSS16].

Careful consideration was put into the formulation of the two scenarios. In the course of developing them, inspiration was taken from this study [23], where one positive scenario was presented, and the participants had to select whether it will or will not happen within 2035. The scenario in [23] concerned human agency in future technology, but the scenarios in the expert and end-user surveys were focused on autonomy and human control in IoT and intelligent environments. The first scenario was positive, stating that humans are able to retain control and benefit from future IoT, whereas the second scenario was negative, stating that humans would lose control and privacy in the presence of IoT. The full formulation of the scenarios can be accessed in Chapter 4.

The reason why the scenarios were formulated in this way is because experts seem to disagree what the future will look like, according to [23], where around half of the expert participants believe humans will lose agency and the other half believe humans will retain their agency to technology in the future. Moreover, as stated in [LS21], it is important to understand what underpins autonomy in addition to protecting it.

Target Groups

The target audience for the expert survey consisted of specialists across various fields. Specifically, the focus was on experts with experience with either IoT, HCI or Human-Centered Design (HCD), or a combination of these, spanning academia, industry, policy-making, and government sectors. This diverse group includes researchers, developers, and policy-makers who can provide valuable insights into the subject matter. Additionally, insights were sought from experts specializing in the social impacts of technology and those adopting a socio-technical perspective, such as sociologists, psychologists, and anthropologists. By involving a multidisciplinary range of experts, the survey aimed to provide a holistic understanding of the topic and its broader consequences.

The target for the end-user survey was to obtain a sample consisting of at least 100 participants and a certain degree of diversity. The aim was a balanced distribution of 50/50 representation of both women and men. Moreover, the sample sought to include a regional representation of 80/20 Norwegians and Western Europeans. Due to time and resource constraints, the sampling had to be based on convenience, which is explained further in Section 3.3.5 [Nik22a].

3.3.2 Questionnaire Design

The questionnaires represent the structured instruments for gathering research data in this thesis. Both surveys were created according to the principles of Roopa and Rani [RR12], and aimed to explore the enablers and barriers to human autonomy in the

IoT through the eyes of experts and the public view. The parts of the questionnaires concerning barriers and enablers were worked out based on a sample of specific factors from the literature review. To survey the end-users, these factors were simplified and various examples were added for context. Extensive pre-testing was performed on both surveys, as per Roopa and Rani's recommendations [RR12]. The surveys were re-iterated several times in collaboration with the supervisors, and they were tested among a selection of technology students from Norwegian University of Science and Technology (NTNU).

Expert Questionnaire

The expert questionnaire is divided into four sections: (1) Demographics and familiarity with the IoT, (2) Defining human autonomy, (3) Potential enablers of human autonomy in the IoT, and (4) Potential barriers to human autonomy in the IoT, as introduced to the participants on the initial page. The two first sections are relatively short, whilst the two final sections are a bit more extensive. The complete questionnaires, both end-user and expert, can be viewed in Appendices E and F, respectively.

To begin with, information about general characteristics was gathered, namely gender, age, and geography were collected. For presenting the profile of the expert panel, i.e., what makes them qualified to be appointed as experts in this study, information was also collected about their education, job title, years of experience, sector they work in, and whether they have contributed to the development or research of IoT or intelligent environment technologies.

The second section contains two open-ended questions where the participants first were asked to provide their interpretation of the term human autonomy in an everyday life context, and then to describe how they believe autonomy manifests in a technical context within the IoT ecosystem. The goal with the use of open-ended questions was to gain insight into the thought processes of those with influence in how IoT technology is developed, and what they believe is important to take into account when designing for autonomy.

In the third section, the participants were first given an open-ended question where they were invited to list any factors they believe can enable human autonomy in IoT, before they were introduced with eleven statements containing enabler factors retrieved from the literature (see Table 4.7. By not suggesting options or predefined answers in an open-ended question, the respondent can reply in their own words and not be constrained by a fixed set of responses [RR12]. This was done with the intention of possibly extracting any new factors that were not identified in the literature review. The participants were requested to answer the open-ended question before proceeding to the next segment, to prevent their answers from being influenced by the list of factors.

Furthermore, the participants were presented with the eleven statements using a matrix question format, which makes use of page space and the respondent's time in an effective manner [RR12]. A matrix question is in reality a set of multiple-choice questions presented in a grid of rows and columns. The rows contain the enabler statements, and predetermined answer options are given in the columns, as shown in the complete questionnaire in Appendix E. The complete list of statements can also be viewed in Table 4.7. The participants were asked to consider each statement, and express their level of (dis)agreement to whether (or not) the factor described contributes to providing human autonomy in the IoT. The aim of this question was to verify the findings from the literature review. The question text explicitly clarified that enhancing or preserving autonomy, agency, empowerment, or control in the context of the IoT represents enabling human autonomy in this questionnaire. To measure agreement, a seven-point Likert scale was employed, spanning from "Strongly disagree" to "Strongly agree," with a "Neutral" option in the center. Additionally, participants were given the choice to respond with "I don't know".

Moreover, the last part of the section aims to assess the enablers' importance for future IoT and give an answer to Research Question 3. With this aim, a positive scenario was presented about what smart environments and the IoT might look like 10-15 years into the future, where humans retain full autonomy in the presence of technology. The participants were then tasked with rating the enabler statements again, but this time concerning the extent to which they believe the factors are important in contributing towards the scenario becoming a reality within 2035. To measure importance, a seven-point Likert scale was employed once more, spanning from "Not at all important" to "Extremely important," with a "Neutral" option in the middle. The participants were also given the option to respond with "I don't know". An optional open-ended question was available, allowing for explanation of the ratings. Lastly, the respondents were instructed to rank the scenario based on likelihood and desirability. For this purpose, two five-point Likert scales ranging from "Very Unlikely" to "Very Likely" and "Very undesirable" to "Very desirable", respectively, were utilized.

The fourth and final section utilized the exact same strategy as the previous section, but with eleven statements containing barrier factors that were retrieved from the literature. First came an open-ended question prompting the participants to list any barriers to human autonomy in IoT, followed by the same agreement rating through a matrix question. For the assessment of the barriers' importance for the future, a different, negative scenario was presented, where smart environments and the IoT is built in a way so that humans lose autonomy. Again an open-ended question was available for explanation of the ratings. Last was the evaluation of likelihood and desirability of this second scenario. On the final page of the questionnaire was an optional open-ended question encouraging the participants to elaborate on any factors related to human autonomy in the IoT they think should be considered in this study.

End-user Questionnaire

The collection of demographic information plays an important role in research studies as it provides valuable insights into the characteristics of the participants involved. The first section of the end-user survey aimed to collect demographic data from the respondents while maintaining their anonymity. The following demographic categories were addressed through multiple-choice questions: gender, age, geography, level of education, and occupation, as well as attitude towards technology. This information was gathered to contribute to the overall analysis and interpretation of the research findings.

The end-user questionnaire is a modified version of the questionnaire used in the expert survey. It is divided into five different sections: (1) Demographics, (2) Familiarity with the IoT, (3) Defining human autonomy, (4) Potential enablers of human autonomy in the IoT, and (5) Potential barriers to human autonomy in the IoT, as displayed to the participants on the initial page. The questionnaire portrays familiarity with the IoT as a separate section instead of incorporating it directly into the demographic section. It differs from the expert questionnaire in having explanations of several concepts such as the IoT, human autonomy, and what an early adopter is. Additionally, the participants were reassured that an explanation of these concepts would be provided in case they were not familiar with the topic.

The following categories were addressed in the demographic section through multiple-choice questions: gender, age, geography, education, and occupation. To begin, participants were asked to indicate their gender and age. Instead of requesting their exact age, age groups were used to ensure anonymity and simplify data processing afterward. Subsequently, participants were asked to indicate the location of their permanent residence. As the survey was conducted in Norway, it was expected that a significant number of respondents would reside in the country. Consequently, Norway was provided as a separate option, distinct from other world regions such as Europe outside of Norway, Asia, North America, etc. Furthermore, participants where inquired about their level of education and occupation, recognizing these variables as significant in reflecting levels of expertise and knowledge. Given the survey's origin at NTNU, a technological institution, it was anticipated that a considerable number of technology students would participate. Hence, including these questions was deemed important.

The second section aimed to examine the participants' attitudes towards new technology and their familiarity with smart technology and the IoT. To achieve this, a matrix question with three statements was utilized. The participants were then asked to indicate their level of agreement to which degree each of the statements apply to them. The statements focus on whether the respondents closely follow emerging technologies, whether they are early adopters of new technology, and whether they are sceptical towards new technology. The intention of these statements was also to be able to differentiate between people who are technically knowledgeable and not, and to facilitate creating segments of those who are especially sceptical towards new technology, to see if they have diverging opinions about factors influencing human autonomy in IoT.

The third section was about the participants' definition of the term 'human autonomy', both in everyday-life and in a technological context. The participants were presented with a multiple-choice question containing three definitions of autonomy to choose from. The definitions are based upon three types of autonomy as described by Dainow [Dai17], and presented in Chapter 2 (see Table 2.1. The types are personal, moral, and political autonomy, as presented in Section 2.3.1 in Chapter 2 of this thesis. The definitions were simplified to easily categorize the understanding of the term among the participants (see Table 4.3). An "I don't know" and an 'Other' option was available, where the latter prompted a follow-up question to allow the respondents to write their own definition of the term.

In the fourth section, the end-users were provided with a modified version of the matrix question about the eleven factors that can be enablers of human autonomy. The statements that were presented in the expert survey are of a technical nature, therefore it was necessary to simplify the phrasing and adjust the statements to be more appropriate for a non-technical audience. Additionally, examples were added in many of the statements to provide context and hopefully give a deeper understanding to those not-so-familiar with the topic (see Table 4.9). Opposite to the strategy in the expert survey, the participants in the end-user survey were first instructed to rate whether they agree that the presented statements are enablers. The same seven-point Likert scale was utilized here as well. The strategy of introducing the factors first was implemented to prevent the participants from becoming overwhelmed with questions about a topic they might not know very well, and potentially drop out. Following the rating was an optional open-ended question where they could point out which factors they think are most important for enabling people to have control over their decisions and actions in the future of IoT.

Identically to the expert questionnaire, the scenario rating was also included in the end-user questionnaire. The same scenario was utilized, followed by a matrix questions where the participants were requested to assess the modified enabler statements according to their importance in contributing to it happening within 10-15 years from now. However, as the questionnaire was already quite extensive, they were not asked to rate likelihood and desirability of the scenario. It was deemed that the experts can be expected to be more qualified to comment on this since they possess specialized domain knowledge and experience of the technology and its development.

The fifth and final section has the same structure as the previous section about enablers, but with the statements containing barrier factors. As before, the statements were simplified to better suit laypeople (see Table 4.11). After rating the statements, the participants were given the opportunity to list the challenges they consider most important to address to make sure humans have control over their own decisions and actions in the IoT ecosystem. Lastly, the second scenario was presented, and the respondents were instructed to rate each barrier according to how important it would be for achieving the scenario. The end page of the questionnaire included an open-ended question encouraging the participants to leave any final comments they might have about the survey or the topic.

3.3.3 Survey Implementation and Operational Aspects

The surveys were published on June 9, 2023, and ran for 31 days, until July 8, 2023. The survey language was English for both questionnaires. The aim was to keep the survey time around 10 minutes, but due to the complicated nature of the topic and the need for explanations of concepts, it may have ended up taking longer. For the expert survey, the aim was 15-20 minutes. The Nettskjema tool was utilized for the technical implementation of the two surveys, for both the creation and execution. All responses are stored in their servers. The anonymous data was also downloaded locally to perform processing and analysis.

Recruitment Strategy

Both participant recruitment and survey invitations were conducted through online channels for the expert survey. Suitable participants for were identified from two sources. Firstly, the list of authors of articles obtained from the systematic literature review was utilized. Secondly, NTNUs expert list[6] was searched using relevant keywords such as "IoT" and "HCI" to find potential domain experts.

A targeted recruitment strategy was employed by contacting a pool of 77 potential participants via email or LinkedIn. Careful consideration was given to the phrasing of each message, ensuring personalized greetings addressing each expert by name and acknowledging their specific expertise. Moreover, in order to expand the reach to

[6] https://www.ntnu.no/eksperter

additional experts, the end-user survey, which was published on LinkedIn, Facebook, and NTNUs internal information channel Innsida, contained a remark encouraging interested experts to reach out via email if they were interested in participating in the expert.

For the end-user survey, both participant recruitment and survey advertisement were conducted through online channels as well. The survey was advertised in a number of channels, namely Facebook and Facebook Messenger, LinkedIn, and NTNUs internal communication channel Innsida. On Facebook and LinkedIn the survey was posted publicly, and in various groups concerned with IoT, ethics in emerging technology such as AI, as well as groups specifically meant for survey-sharing. On Innsida, the survey was shared with everyone in the Communication Technology and Digital Security (MTKOM) study program, a bulletin board for recruiting participants to research studies, and all Ph.D. students in the Information Security and Communication Technology program. The survey invitation that was used can be viewed in Appendix D. Additionally, the survey was advertised on the two online survey-sharing platforms SurveyCircle[7] and SurveySwap[8].

Data collection and privacy

Both surveys were designed to ensure complete anonymity of all participants, adhering to Nettskjema's checklist for anonymity safeguards[9]. Participants were never required to disclose any personally identifiable information (e.g., name, age, phone number, address, social security number, etc.) or sensitive process data (e.g., IP address, e-mail address, browser cookies, etc.) that could be traced back to them. Furthermore, confidentiality was maintained throughout the handling and storage of all collected data. This explicit assurance of anonymity and confidentiality was communicated to the participants on the survey's initial page.

3.3.4 Processing and Data Analysis

All data from both questionnaires were downloaded on July 8, 2023, after closing off the online surveys for participation. The data was structured as an Excel file with a complementing codebook. The questions were coded into columns, and each cell in the column contained an integer value according to the answer options for the particular question. The mappings between questions and columns, and answers and integers, were provided by the codebook. The reason for using integers instead of the actual answers is to make data processing in Excel simpler and more convenient.

[7] https://www.surveycircle.com/en/

[8] https://surveyswap.io

[9] https://www.uio.no/tjenester/it/adm-app/nettskjema/hjelp/tiltak-for-a-sikre-anonymitet.html

Descriptive analysis was performed on both datasets to summarize the results. An overview of the characteristics of the participant samples can be found in Chapter 4, see Sections 4.2 and 4.3. A number of graphs and charts were created to illustrate the results of the different ratings of statements. These mostly include diverging stacked bar charts and 100% stacked bar charts, but also tables depicting the calculated average scores and standard deviation. Moreover, open-ended questions were coded manually in Excel with the aim of identifying recurring themes. Specific examples are presented as quotes from the open-ended questions.

3.3.5 Survey Limitations

The following section outlines the identified limitations of the survey methodology used in this thesis. These limitations include structural constraints, general drawbacks associated with data collection through surveys, biases, and specific limitations pertaining to elements derived from the Delphi method.

Structural and General Limitations

The surveys exhibit certain structural limitations that should be acknowledged. Firstly, the phrasing of questions in the end-user survey introduces a potential limitation. A decision was made to include examples for a lot of the questions, in an effort to make the technical descriptions more tangible for the consumers, in case they were unfamiliar with the topic. However, it might have lead to the statements becoming longer and more complex, and thus more difficult to read and understand for laypeople.

Secondly, the use of incorrect terminology presents another limitation. The phrase 'i.e.,' derived from the Latin 'id est,' meaning 'that is,' was wrongfully utilized throughout both surveys with the mistaken belief that it meant 'in example'. The correct term is 'e.g.,' derived from the Latin 'exempli gratia,' which translates to 'for example.' This misuse may have contributed to confusion and misunderstandings regarding the questions posed.

Survey research, as discussed by Decarlo [DeC18], is also subject to general limitations. One limitation is the inherent inflexibility of surveys, whereby questionnaires cannot be altered once they have been distributed. As previously mentioned, the technical and complex phrasing of questions in the end-user survey may have led to participant misunderstandings. Unlike in an interview setting where clarifications can be provided [DeC18], this lack of opportunity for further elucidation may have resulted in erroneous responses. To try and minimize this limitation, pre-testing of both survey was performed before they were published.

Furthermore, the standardized nature of questionnaires can lead to lack of depth in the collected data [DeC18]. To address this limitation, the surveys in this thesis include optional open-ended questions. These questions are designed to elicit more comprehensive insights into participants' reasoning, beyond what multiple-choice questions can provide.

A limitation of the recruitment strategy relates to the use of survey sharing websites to recruit participants. While these platforms offer a convenient means to access a broader pool of potential respondents, they introduce certain challenges that can impact the reliability and validity of the collected data. One noteworthy limitation is the external incentive system, wherein participants receive points or rewards for each survey completed. This incentive structure may lead some individuals to prioritize quantity over quality and rush through surveys in pursuit of rewards, potentially compromising the accuracy and truthfulness of their responses. Moreover, the presence of external incentives may create a bias towards participation by individuals who are primarily motivated by the rewards rather than genuine interest in the research topic. This could result in a skewed sample, potentially lacking in the diversity and representativeness necessary for drawing meaningful conclusions. Additionally, the anonymous nature of these survey sharing websites may make it challenging to ensure the authenticity of responses. The lack of direct oversight or personal accountability might encourage participants to provide insincere or careless answers, further compromising data integrity. This particularly pertains to those participating through the survey sharing websites, as it is easier to control who is exposed to the survey in the other channels mentioned.

Finally, the Delphi and Foresight elements posses some inherent limitations. According to [FDD+19], the Delphi survey has no single agreed-upon methodology. It can seem somewhat abstract, and there is a lack of guidance and agreed standards in the literature, which can lead to the researchers having to make assumptions without having an established methodology to point to. Due to this, it is difficult to know whether the results are reliable or not, and the future perspective makes it hard to measure their reliability [SNCL15].

N.B.: It was discovered that only 40 out of the 41 articles were included in the SPSS analyses. Since this was discovered so late in the project, there was no time to do it over again, so the results are based on the original analyses.

Biases

As with all research, the surveys are susceptible to biases. This is important to take into account when attempting to generalize the findings, and when interpreting and discussing the results and their validity. One type of bias that can occur in surveys is selection bias: systematic error related to the survey's participants, for instance introduced during selection of population, sampling, or recruitment [Nik22b]. Sampling bias is a type of selection bias that happens when certain individuals or elements in a population have a higher chance of being selected for a sample compared to others [Bha20]. This systematic discrepancy in the selection process can make the sample unrepresentative and affect how well the research findings can be applied to the broader population. Three examples of sampling bias are self-selection bias, nonresponse bias, and undercoverage bias [Bha20].

Self-selection bias is when people with certain characteristics are more likely to agree to participate in the survey than others, while nonresponse bias is when those who drop out or decline to participate in the survey display systematic differences compared to those who choose to take part [Bha20]. These biases may have occurred in the end-user survey; the technical nature of the language used may appeal more to academics and people with an interest in smart technology, than laypeople, who may have been inclined to not participate or drop out due to this. To mitigate this, several measures were implemented. Consideration was given to the creation of the title of the survey to avoid discouraging those not-so-familiar with the topic. In the initial page of the questionnaire, it was emphasized that relevant terms and concepts would be explained later. Most importantly, efforts were made to phrase the statements about barriers and enablers in as simple and easy-to-understand terms as possible, and to avoid it becoming too long and complicated. Nevertheless, the topic at hand is a complex one, making it challenging to understand for people with little experience with smart technology, as well as challenging to phrase the questions in a simple and straightforward manner.

Undercoverage bias is introduced when certain members of a population are entirely omitted or excluded from the sample frame employed in a study [Bha20]. This can happen through the use of convenience sampling, which is when "participants are selected based on accessibility and availability" [Bha20]. One example of an excluded group can be elders and those without access to the Internet. Due to both time and resource limitations, convenience sampling was used as the sampling method in this study. Since the survey was published to NTNU's internal network, the author's social network, and the supervisor's professional network, it was exposed to a lot of students and academics, which does not reflect the actual population. This also goes for the survey sharing websites it was published to, since they are mainly used by students and researchers for research purposes. However, the recruitment strategy is described in detail in Section 3.3.3 to make it reproducible and replicable, which can reduce bias [Nik22a].

Chapter 4 Results

This chapter presents the findings from the systematic literature review and the expert and end-user surveys. It consists of three sections, respectively, that are constructed in a similar way. The results from the literature review are presented in 4.1. First, general characteristics are described, followed by interpretations of 'human autonomy' found in the literature, and finally an overview of the identified enablers and barriers that can influence human autonomy in the IoT. Next are the results from the expert and end-user surveys in sections 4.2 and 4.3. Both sections have a description of the sample, their understanding of the term 'human autonomy', and finally an assessment of the identified enablers and barriers. Section 4.2 also includes the experts' judgement on likelihood and desirability of the scenarios that were presented in the surveys.

4.1 Results from the Literature Review

The key objectives for the literature review results were to contribute towards achieving Research Questions 2 and 3 (see Section 1.2), and to the identify areas that required further research in the quantitative expert and end-user Delphi-inspired studies. This included a mapping of the status of technical solutions in use, and the barriers and enablers towards protecting human autonomy in IoT.

First, the literature review synthesis grouped the articles by their general characteristics as described in Chapter 3 (see Table 3.1), such as year, the publication type, geography, author perspective and expertise. Then, the design approach, the theory, framework, and outcome was categorised. Finally, the technical and non-technical factors were identified and labelled. A labelling of each factor's inhibiting or enabling qualities were assigned, followed by gaps for future research.

4.1.1 Description of Articles

Table 4.1 presents the general characteristics of the articles that were included in the systematic literature review. A complete list of the articles (n=41) can be viewed in Appendix C, see Table C.1. As mentioned in Chapter 3, no limitations were set in terms of time of publication when searching for literature. However, there seems to have been an distinct increase in focus on the topic since 2016, seeing as 70% of the articles were published after this time. There is also a pattern to be observed with regard to geography, as most of the articles originate from Europe (60%) and the Western world (27.5%), and only 12.5% in other parts of the world. When it comes to publication type, the search yielded half journals and the other half conference proceedings, with the exception of 5% of the articles which were book chapters. Technology is the most prominent field, with half of the authors having their expertise within it, but that means social sciences and humanities are not far behind, constituting the other half. It can also be observed that taking a multidisciplinary approach to the research of this topic is more prevalent than a single-discipline point of view.

Table 4.1: General characteristics of articles in the literature review.

Characteristics	Category (percent)
Year	2001 – 2016 (30%), 2017 – 2023 (70%)
Geography	Europe (60.0 %), North-America (20.0 %), Africa and Middle East (10.0 %), Australia (7.5 %), Asia (2.5 %)
Publication type	Conference proceedings (45.0 %), Journals (50.0 %), Book chapter (5 %)
Expertise	Technology (50.0%), Social science (32.5 %), Humanities (17.5 %)
Perspective	Multi-discipline (62.5 %), Single (37.5 %)

4.1.2 Defining Human Autonomy

The article set was analyzed in terms of theories and frameworks utilized for achieving different human-centered outcomes. Table 4.2 summarizes the theories and frameworks, and the articles' intended human-centered design outcomes. The table reveals that as much as 37.5% of the articles don't explicitly state the theory that supports the design principles. 47.5% of frameworks are centered around designing for humans or society, while 45% are concerned with the sensing system's technical capacities. The last 7.5% focus on legal capabilities, for instance and other regulatory frameworks.

Table 4.2: Human-centered theory and frameworks utilized in the articles from the literature review.

Design principle/approach	Category (percent)
Theory	Explicitly stated (62.5 %), Not explicitly stated (37.5 %)
Framework	Humanistic (47.5 %), Rational (45.0 %), Judiciary (7.5 %)
Design outcome	Control (40.0 %), Empowerment (20.0 %), Autonomy (17.5 %), Privacy (12.5 %), Security (5.0 %), Other (5.0 %)

To query end-users about their interpretation of human autonomy, there was a need to come up with categorizations of different definitions. For this purpose, the definitions from Chapter 2 by Dainow [Dai17] were used (see Table 2.1). These definitions of personal, moral, and political autonomy were then simplified to be used in the survey, resulting in the paraphrased statements shown in Table 4.3.

Table 4.3: Question statements to categorize perceptions of autonomy [Dai17].

Definition	Question statement
Personal	My ability to be in control of my own life.
Moral	Feeling empowered to determine my own path and live according to my own values.
Political	The ability to make individual choices freely, without being restricted by others or dictated by technology.

Figure 4.1 illustrates the articles according to their primary human-centered design outcome and year of publication. From the figure it is clear that all the outcomes have gained recognition since 2016, emphasizing what was mentioned above about how 70% of the articles were published after this time. According to both Table 4.2 and Figure 4.1, control is the outcome which has been most focused on in total. Nevertheless, more attention is being directed towards autonomy and empowerment in IoT in recent years, as well as to security and privacy.

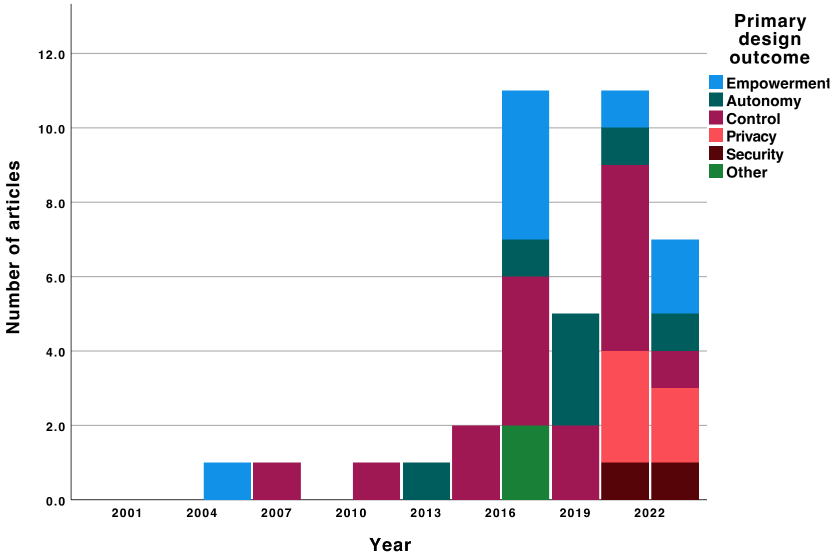


Figure 4.1: Articles targeting human-centered outcomes.

4.1.3 Enablers and Barriers

During the analysis of the literature, it became apparent that enablers and barriers in many cases are two sides of the same coin. For example, an enabler of human autonomy in IoT would be to be able to give explicit consent to various types of data collection and use techniques of the IoT devices, but a barrier can be the IoT's limited support for the exercise of informed consent [BCRW17]. Therefore, the barriers and enablers that were identified in the systematic literature review are listed more neutrally, simply as factors, as seen in Table 4.4. Ultimately, Table 4.4 contributes to achieving Research Question 2. In the table, each factor is coded with a capital F (for factor) and a number between 1 and 20, with the associated references where they were extracted in a separate column. The "Statement" column links the factors to the statements that were used to describe enablers and barriers in the surveys. The enabler and barrier statements are coded with a capital E or B, respectively, and a number between 1 and 11, to refer to the enabler statements in Tables 4.7 and 4.9, and barrier statements in Tables 4.8 and 4.11.

The factors warranted inclusion in Table 4.4 if they were defined in the literature as something influencing autonomy, agency, empowerment or control. For example, surveillance threatens autonomy directly [Dai17]: Implementing IoT devices and sensors in all parts of the environment opens up the possibility for non-stop, involuntary and ubiquitous monitoring of individuals [FS15]. Some of the factors encompass several aspects. One example is F4, where there are a number of underlying factors such as the lack of interoperability between devices due to heterogeneous protocols and proprietary systems [Dai17; DAM17].

As can be observed in Table 4.4, some of the factors listed are not linked to any survey statements. First is self-monitoring (F1.5), which can be said to be related to surveillance (F1). The choice was made to exclude this from the surveys because it is more niche than the other factors, and thus out of scope for this thesis. It concerns how HIoT wearables, the IoT devices themselves, provide patients with more agency and empowerment through use [FAMC22; PZ21], and not how aspects related to human autonomy can be technically translated into the IoT. Factors F10 (privacy) and F12 (anonymity) were deemed to be similarly themed as F11 (security), which is not the main focus in this thesis as there seems to be lot of research already happening in these areas. F18 (context-awareness), F19 (competence/education), and F20 (trade-offs) were identified in the literature after the surveys were published, and were therefore not addressed through the questionnaires. However, F19 was identified by both the experts and end-users in the open-ended questions, see Sections 4.2 and 4.3. Context-awareness (F18) is also related to surveillance (F1), so it can be said to be covered by F1.

Out of the factors that were identified in the systematic literature review, a selection was used to produce eleven enabler statement and eleven barrier statements. These statements were utilized in the expert and end-user surveys to query the participants about their perception of how important the enablers and barriers will be to human autonomy being preserved or lost in future IoT. Sections 4.2 and 4.3 present the results from the expert and end-user survey, respectively.

Table 4.4: Factors identified in the systematic literature review.

Code	Factor	Statement	Reference
F1	Surveillance	B1	[Dai17], [BCRW17], [BBNT18], [FS15], [SHK+21]
F1.5	Self-monitoring		[FAMC22], [PZ21]
F2	Disparity of control	B2, B3	[Dai17], [RM06], [BCRW17], [DAM17], [CCFS16], [PZ21], [JKH20]
F3	Configurability	B4, B5, B9	[Dai17], [AF15], [DAM17], [JCP17], [OS22]
F4	Variation in operational models	B6	[Dai17], [DAM17], [BCRW17]
F5	Customization	E1	[BCRW17], [HWJ20], [DAM17], [BBNT18]
F6	Transparency	E3, B10	[BCRW17], [AF15], [SCD22], [SCN19], [BBNT18], [OS22], [BEG+17]
F7	Personalization	E2	[AF15], [STHK20], [BBNT18], [BLY13], [SPKZ21], [NO16]
F8	Accessibility	E4, B11	[KZDB19], [DAM17]
F9	Accountability	E11	[SCN19], [BBNT18]
F10	Privacy		[BBNT18], [Dim16], [OS22]
F11	Security	E10	[CDMR19], [HS20], [JCP17], [PZ21], [Dim16], [SS22], [MKAB19], [PFH15]
F12	Anonymity		[SCD22]
F13	Simplicity	E5	[SCD22], [ZAD20], [BEG+17]
F14	(Explicit) consent	B8, E8	[SCD22], [BCRW17], [OS22]
F15	Legal frameworks	E6, B7	[SCD22], [BCRW17], [SCN19], [BBNT18], [FS15], [GVK19]
F16	User interface/H2M communication	E9	[RJJ+22], [HWJ20], [YH21], [Kur21], [DAM17], [Röc10]
F17	Design frameworks	E7	[KZDB19], [DAM17], [BBNT18], [GVK19], [AJD+16], [OS22], [CGM+21]
F18	Context-awareness		[OS22], [SPKZ21], [BBNT18]
F19	Competence/education		[OS22], [Eco17]
F20	Trade-off utility vs. privacy		[BBNT18], [OS22], [LBC18]

4.2 Results from the Expert Survey

The objective of the expert survey was to investigate expert interpretations of autonomy as a term, and assess the barriers and enablers identified in the literature review from an expert point of view, and together with the end-user survey contribute towards providing an answer to (RQ1), RQ2, and RQ3. The section follows a similar structure as the one above. First, a general description of the expert panel is given. Secondly, examples of definitions of human autonomy provided by the participants are presented in the form of direct quotes from the survey. Thirdly, the results from the evaluations of enablers from the literature are presented, accompanied with any new factors as identified by the experts. Lastly, the same is done for the assessment and identification of barriers.

4.2.1 Panel Description

Table 4.5 gives an overview of the panel of twelve experts who participated in the expert survey. Each participant has been given a code consisting of a capital X combined with a number between 1 and 12, so that quotes or answers given can easily be referred back to this table throughout the rest of the chapter. The experts are listed according to their job title, industry segment, gender, and years of experience. The column marked with an asterisk (*) describes whether they have developed or contributed to the development or research of IoT or intelligent environment technology. As indicated in Table 4.5, all but one of the experts are from the public sector. When it comes to gender, all are male but one. The participants are all quite experienced, and familiar with IoT, as 2/3 of the panel has 10 or more years of experience, and 10 out of 12 have worked with IoT or intelligent environment technology.

4.2.2 Autonomy

This section presents the results from section 2 of the expert survey, two open-ended questions about the definition of autonomy (see Appendix E for the exact questions). The participants provided definitions of human autonomy that can go into the categories personal, moral, and, political from Table 4.3 in the previous section. Table 4.6 introduces an example each of personal, political, and moral autonomy, as described by the experts. The table also includes one statement that differs a lot from the rest, questioning the absolute nature of human autonomy, categorized as "Other".

Analysis of the results demonstrates that the personal autonomy definition was most dominant among the experts. In section 4.3, there is a bar chart (Figure 4.13) comparing the experts' definition to the end-users'.

Table 4.5: Profile of expert panelists.

Code	**Job Title**	**Industry Segment**	**Gender (M/F)**	**Experience (years)**	*
X1	Senior Research Fellow	Private	Male	5-10	No
X2	Associate Professor	Public	Male	10-15	Yes
X3	Associate Professor in Human-Centered Computing	Public	Male	15-20	Yes
X4	Full Professor	Public	Male	20+	Yes
X5	Associate Professor in Computing	Public	Male	20+	Yes
X6	Professor in HCI	Public	Male	20+	Yes
X7	Professor	Public	Male	20+	Yes
X8	Instrumentation Engineer	Public	Male	1-5	Yes
X9	Associate Professor in Industry 4.0/Sustainable Manufacturing	Public	Male	5-10	Yes
X10	Researcher, Social Science	Public	Female	1-5	No
X11	Associate Professor in ICT	Public	Male	15-20	Yes
X12	Associate Professor	Public	Male	15-20	Yes

In the open-ended question about how human autonomy manifests technically in the IoT ecosystem, the experts described several ways this can happen. Staying in control of the devices and their data collection was mentioned several times, by X3, X5, X8, and X12. This corresponds to the definition of personal autonomy in Table 4.3. X3 also had a second definition: human autonomy can by achieved by setting up and managing an IoT ecosystem is such a way that it does what the user wants, either through direct control or automation. This corresponds to the system extending human autonomy as described by Dainow [Dai17].

Transparency was also a recurring theme, brought up by X7, X8 and X12. X7 and X8 placed emphasis on the availability of information, as well as informed decision-making. X12 highlights that the system should not hide information or make unwanted decisions on behalf of humans. Furthermore, the use of human-centered design frameworks for the development of IoT devices was a theme expressed by X8 and X9, underlining that humans/users and their needs should be in the center to facilitate autonomy when developing and implementing new technology. X11 stated that IoT can enable human autonomy through additional access to knowledge and innovative accessibility solutions, but points out its ability to accentuate social gaps

Table 4.6: Experts' definitions of human autonomy in an everyday life context.

Expert	**Statement**	Category
X12	To which degree a human can make decisions about the things that do or should concern them.	Personal
X10	Human autonomy for me is the ability to act, think and exist without others (material, societal) interfering or steering these practices.	Political
X6	It is the idea that people are free to make their own decisions and are empowered to take the actions that advance their interests / goals. It is partially related to freedom (from restrictions) and partially related to empowerment (having options and abilities).	Moral
X1	We are in no way separate, independent, or autonomous, but we are deeply inclined to believe otherwise–just as we believe we are substantial rather than mostly space.	Other

between those with access to education and economical power and those who are not "favored" to receive this potential additional autonomy. This phenomenon is called the Digital Divide [LSE22].

Several new perspectives on human autonomy in the IoT that were not identified in the literature, appeared from this question. First is X6's way of classifying it as either "freedom from" or "freedom to":

> *There are probably two major ways to think about this. One is how IoT might constrain or limit or unduly influence one's behaviors in negative ways. For example, certain kinds of nudges or dark patterns to change people's attitudes and behaviors, privacy concerns such as surveillance (e.g. young children in homes or workers in offices), safety (e.g. intimate partner violence), and limitations on computing (e.g. DRM). These are all examples of "freedom from". The other way to think about IoT is enabling technologies that can augment and/or improve people's lives, e.g. aging in place, helping people with assistive needs. These are all examples of "freedom to".*

For information, DRM, or digital rights management, uses technology for controlling and managing copyrighted material, relieving the material's owner of this responsibility [Roa23].

Secondly, X1 had the following description, again questioning the true nature of autonomy:

> *Human autonomy manifests as relatively unpredictable processes, from the human standpoint, when compared to the processes of simpler, human-conceived systems. In reality, human autonomy is the product of chains of causation, as is every other development which comes into being. It will one day be possible for AI to identify all of the separate factors which bear on human experience. Then, we, too, will be revealed to be quite predictable, with access to the right data and analytical capabilities.*

Finally, X4 stated that the intelligent system provides humans with autonomy through technical features such as AI and machine learning, whereas X3 declared that autonomy does not manifest at all in the IoT ecosystem.

4.2.3 Enablers

The following section presents the results from section 3 of the expert survey, with reference to the specific questionnaire in Appendix E. Firstly, the qualitative data from the open-ended question about enablers is introduced, accompanied by the quantitative data from the rating of enabler statements. Finally, their assessed importance for future IoT is presented.

The experts were asked to list any enablers of human autonomy they could think of in an open-ended question, before they were faced with the set of enablers from the literature. Some of the replies contained factors that were also identified in the literature review. These include user-friendly and intuitive interfaces, alerting users of the status of the IoT system, transparency, involving humans in the design and development processes (e.g., through HCD and understanding the socio-cultural context), privacy, security, interoperability between devices and compatibility across platforms, personalization and context-awareness, end-user awareness, and legal frameworks to enforce these features.

Some of the particulars that were mentioned by the experts are related to the factors from the literature review, but not quite the same. One example, as mentioned by X6, is platform regulation. To put it into context, X6 draws a parallel to regulation of iOS and Android platforms, underlining that similar regulation of IoT platforms will be relevant in the future since corporations will want to be THE platform that everyone uses. Another example, as declared by X8, pertains to legal frameworks. More specified, international legal frameworks that allows owners of a device to control what firmware the device is using at all times, and to ensure that the user can maintain an repair the firmware if the manufacturer's support ends. According to X8, this empowers the user even if they are not skilled within IoT:

> *These legal frameworks empower the user to take control of the life-cycle of a device, to decide when a device is considered to be obsolete, and to decide what the purpose and functionality of a device should be. These legal frameworks can seem to only benefit those individuals that have the necessary skills to reconfigure electronic devices, but the Open-source movement has shown that this will also benefit users with a minimal skill-level.*

However, the experts also came up with some aspects that were not identified in the literature review. These include democratic involvement of citizens in deciding if, when, and how IoT is used and what goals and values to pursue with the technology.

Expert evaluation of Factors Found in the Literature Review

From the factors identified in the literature review (see Table 4.4), a set of enabler statements was created. Table 4.7 lists these statements as they were worded when presented to the participants in the expert survey.

Figure 4.2 is a diverging stacked bar chart, illustrating the experts' level of agreement to whether the presented statements describe mechanisms that enable human autonomy in today's IoT. The statements are mapped using a capital E (for enabler) and a number between 1 and 11 (i.e., E1, E2, etc.), where the codes refer to the statements in Table 4.7. The chart employs a divergent color scale spanning from bright red to bright green to illustrate the spectrum of agreement levels, ranging from "Strongly disagree" to "Strongly agree." The percentage distribution of responses for each enabler statement is depicted using both color mapping and labeled percentages. The participants were also given the option to choose "I don't know" as an answer; this option was only selected twice, once in E8 and once in E9, and was therefore omitted from the chart in Figure 4.2.

From Figure 4.2, it is evident that E3, E4, E5, and to some degree E10, are most agreed upon to be enablers of autonomy. E3, E4, and E5 all have a high percentage of participants saying they strongly agree, with a rate of 50% or more, whereas E10 has 41.7% strongly agreeing. These results validate what was found in the literature review, answering Research Question 2. The results indicate that the experts place most importance on transparency (E3), accessibility (E4), and designing privacy policies that are easy to understand (E5). Security (E10) has a high percentage who strongly agree to this as an enabler, but a significant of participants also said they are neutral towards the statement or somewhat disagree with it. Furthermore,

Table 4.7: Enabler statements presented to the participants in the expert survey.

Code	**Statement**
E1	Allowing users to customize machine-to-machine automation between IoT devices, i.e., by the use of End User Development methods.
E2	Personalized privacy recommendations for data sharing and processing in IoT.
E3	Transparency and explainability of IoT systems, allowing users to understand how their data is collected, processed, and used.
E4	Accessibility for users with impairments, i.e., a configurable user interface that presents different levels of interaction corresponding to the levels of a user's abilities.
E5	Designing privacy policies that are easy to understand.
E6	Regulations and legal directives such as GDPR.
E7	The use of frameworks such as privacy-by-design and value-sensitive design when developing IoT systems.
E8	System sends nudges or notifications that warn users of risk-averse situations, i.e., when they are about to share personal data.
E9	Providing innovative interaction strategies for human-to-machine communication, i.e., voice command, user-friendly interfaces.
E10	Improved information security and communication network security.
E11	Clear conveyance of accountability in complex IoT systems and systems-of-systems.

statements E1 and E2 have a high percentage of participants who said they are neutral towards them. This indicates that customization (E1) and personalized privacy recommendations (E2) may not make much of a difference in protecting autonomy.

In Figure 4.2, E8 stands out with the highest percentage of disagreement, as 33.3% of the responses were "Somewhat disagree". This indicates that there is divergence of opinions regarding whether notifications from the system about risk-averse situations (E8) genuinely facilitate autonomy in the context of IoT. The chart, Figure 4.2, also demonstrates that the responses are distributed across the agreement scale in all statements, signifying a range of perspectives among the experts. While there is some level of disagreement among the experts about the classification of the statements as enablers, it is noteworthy that none of the participants expressed strong disagreement with any of them.

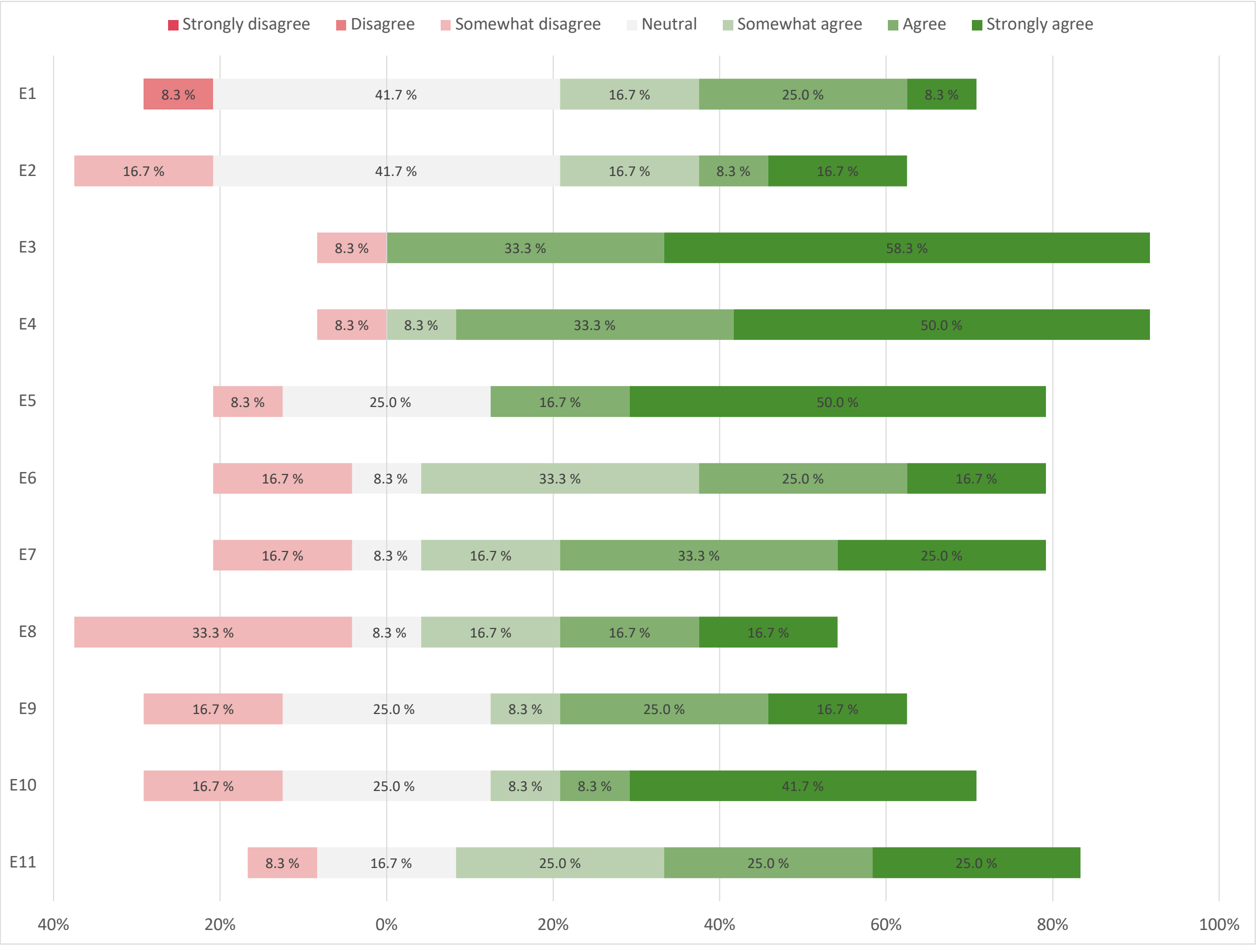


Figure 4.2: The expert panel's level of agreement to whether the presented statements are enablers of human autonomy in IoT.

Assessing the enablers' significance for future IoT (RQ3)

To provide an answer to Research Question 3 and assess the significance of the enablers for future IoT, the following scenario was presented in the survey, and the participants were asked to rate each statement according to how important it will be for achieving the scenario within 2035.

> **Scenario 1**: By 2035, smart environments and IoT will allow humans to retain full agency over IoT systems, enjoying the benefits of automation, connectivity, and efficiency while maintaining control over their own lives.

The results of the assessment of the enablers are illustrated in Figure 4.3, a 100% stacked bar chart where each bar represents an enabler statement, mapped using the E1 through E11 codes to refer to Table 4.7. The chart employs a somewhat modified single hue scale spanning from dark blue to light blue, where the darkest blue signifies "Not at all important", and the brightest signifies "Extremely important". Neutral is marked in gray to more easily distinguish the lower and upper parts of the scale in the figure. The "I don't know" answer option is added in the far right of the chart, colored light orange. Labels with the percentage of participants who gave that answer are added to each bar for clarity.

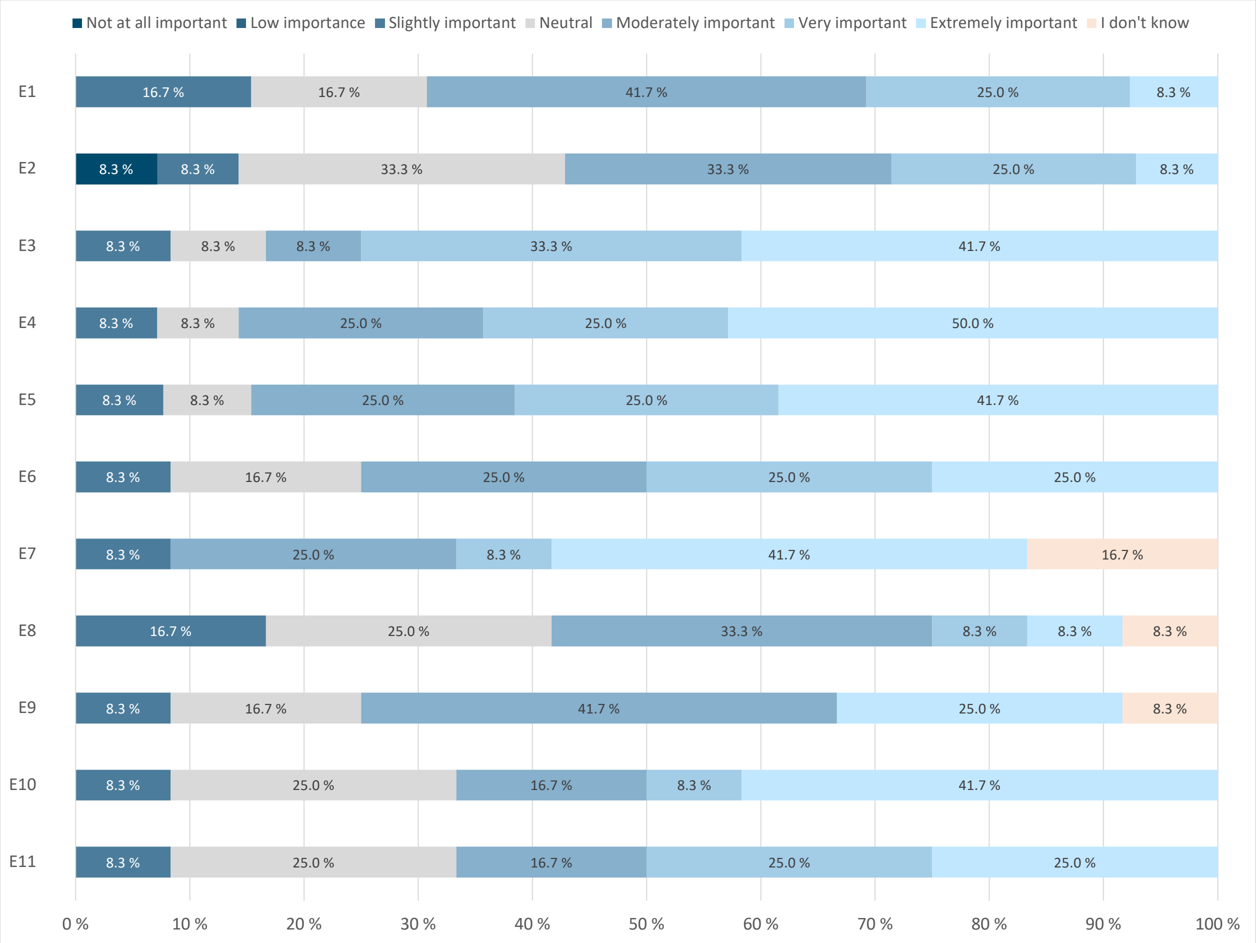


Figure 4.3: Stacked bar chart depicting the importance levels assigned by the expert panel to the presented enablers for achieving Scenario 1 in the future of IoT.

From Figure 4.3, it looks like the expert panel deems E3, E4, E5, and E10 the most important enablers for achieving Scenario 1. This is also reflected by their agreement levels in Figure 4.2, where these enabler statements have the highest percentages of "Strongly agree" answers. However, in Figure 4.6, E10 has 25% neutral answers, which indicates that some participants don't think it will impact autonomy in the future as much. The same goes for E2, E8, and E11, which have one-fourth or one-third neutral answers. This indication is supported the responses to the open-ended follow-up question, where the experts were given the opportunity to elaborate on their importance ratings. X2 sees privacy and security as separate issues from autonomy, while X1 wrote the following about the "Neutral" answer option:

> *Where my answers are neutral, it's because I don't think this will necessarily give people what they want. People want to feel free of interference or unwanted influence, but when you require that they do something, you create an obligation which potentially infringes upon their sense of autonomy.*

It can be noted that only one of the statements, E2, had an answer that say it is "Not important at all". All the other statements are "Slightly important" or higher on the scale. The average importance score along with the standard deviation of all the enablers have been calculated to compare with the end-users' scores in Section 4.3 (see Table 4.10 specifically).

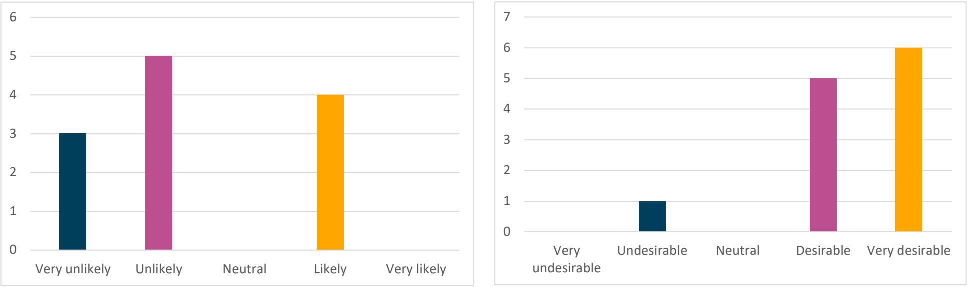
X3 stated in a comment that usability is most important in a system compared to other factors:

> *I think that usability is really important. It is one thing for a system to be highly configurable... usually such systems are too complex for most users to understand. A system that truly supports human autonomy helps the user translate their goals/desires into system settings (cf. Don Norman: bridge the gulfs of execution and evaluation).*

Moreover, X10 had the following to say about the enablers, shedding light on some of the implications of designing the survey in the way it has been done:

> *I think none of the abovementioned is doing anything in isolation. These suggestions all also fail to address power and capitalism as important factors shaping technology design. I can see a clear "techno-solutionism" in these suggestions build on the assumption that IoT actually will benefit society. Many of the suggestions are also focusing on individual, rather than collective ways of interacting with technology in society.*

Finally, Figure 4.4, comprised of two bar charts, summarizes the the experts' opinions on the the likelihood and desirability of Scenario 1. Figure 4.4a illustrates the experts' anticipated likelihood of Scenario 1 becoming a reality within 2035, and Figure 4.4b depicts how desirable they find it, regardless of viability. Figure 4.4 shows that generally, there is agreement that the scenario is desirable, but some disagreement about the likelihood of it. One-third of participants find it likely, whereas the rest find it unlikely or very unlikely.



(a) Likelihood of S1.

(b) Desirability of S1.

Figure 4.4: Two bar charts depicting the experts' judgement of the likelihood and desirability of Scenario 1.

4.2.4 Barriers

This section presents the results from section 4 of the expert survey, see Appendix E for the specific questions. Firstly, the qualitative data from the open-ended question about barriers is introduced, followed by the quantitative data from the rating of enabler statements. Finally their assessed importance for future IoT is presented.

The participants were asked to list any barriers to human autonomy they could think of in an open-ended question, before they were faced with the set of barriers from the literature. Some of the replies contained factors that were also identified in the literature review. These include security and privacy risks, bad user interfaces and systems, third-party interest in surveillance and control, monopoly-tendencies, money-driven incentives instead of user-centered incentives for development of technology, lack of compatibility and interoperability, inadequate and slow legislation, biased and opaque algorithms, trade-off between utility/usability and other aspects such as configurability, and market, organizational and institutional structures. The issue of insufficient education and awareness was also raised. As stated previously, this was identified in the literature, but not included in the surveys.

Some of the particular aspects that were mentioned by the experts are related to the factors from the literature review, but not quite the same. One example, as brought up by X9, is the power given to global tech:

> *Obviously, human use of "free" data platforms like Facebook, Google has given "global tech" too much power - which is likely too valuable for these global actors to give up easily.*

Another point was made by X1 about the paternalistic and persuasive behavior of technology.

> *The leveraging of data for influence/persuasion: people may be led into situations that they ultimately would rather not be in.*

Analogous to this, X1 also brought up conditioning, and how "people may be intentionally influenced through presented stimuli or messaging, or even by virtue of design elements in an environment". Manipulation and persuasion from systems did note come up in the systematic literature review, but was discussed in part in the project proposal [Lei23]. X1 also questions human capacity, describing it as limited, and that people do not necessarily understand what they want and how to get it.

Moreover, the experts also brought attention to two aspects that were not identified in the literature review. These include ignorance among the public and the lack of proper tools to build systems in an autonomy-preserving manner.

Expert Evaluation of Factors Found in the Literature Review

From the factors identified in the literature review (see Table 4.4), a set of barrier statements was created. Table 4.8 lists these statements as they were worded when presented to the participants in the expert survey.

Figure 4.5 is a diverging stacked bar chart, illustrating the experts' level of agreement to whether the presented statements describe mechanisms that inhibit human autonomy in today's IoT. The statements are mapped using a capital B (for barrier) and a number between 1 and 11 (i.e., B1, B2, etc.), where the codes refer to the statements in Table 4.8. The chart employs a divergent color scale spanning from bright red to bright green to illustrate the spectrum of agreement levels, ranging from "Strongly disagree" to "Strongly agree." The percentage distribution of responses for each barrier statement is depicted using both color mapping and labeled percentages. The participants were also given the option to choose "I don't know" as an answer; this option was only selected four times, once each in B3, B4, B5, and B9, and was therefore omitted from the chart in Figure 4.5.

Table 4.8: Barrier statements presented to the participants in the expert survey.

Code	**Statement**
B1	Third-party interest in gathering information from personal intelligent environments (surveillance).
B2	Third-party interest in seeking control over personal environments.
B3	Lack or concealment of user configuration capabilities in IoT devices.
B4	Limitations in configurability of IoT, restricting the user's options to predetermined pathways created by programmers.
B5	ICT developers not recognizing the need for variations in development of IoT devices.
B6	Dependence on centralized authorities and service providers, potentially leading to data monopolies.
B7	The speed of the evolution of IoT is outpacing regulatory processes, potentially impairing effectiveness of regulations.
B8	Limited support for ensuring informed consent in IoT, i.e., giving users the opportunity to accept or oppose data collection and use.
B9	Systemic biases, i.e., in business models, market competition, regulatory frameworks or any other aspects regarding the operational delivery of services.
B10	Users do not have complete information about consequences of disclosing data, i.e., systems' collection of position data.
B11	The Digital Divide – unequal access to technology (such as IoT) in society, potentially disadvantaging part of the population.

In general, as indicated by the agreement level about barriers in Figure 4.5, there is more consensus among the experts on the barriers to autonomy in the IoT, than there is on the enablers. Compared to the prior stacked bar chart (see Figure 4.2), the answers are less distributed across the agreement scale, and there is clearly a preponderance of responses in the agree range. This applies to all eleven statements, as between 66% and 100% of the answers are either "Somewhat agree", "Agree", or "Strongly agree", in every case. Noticeable are statements B2 and B5, in which none of the answers are on the disagree range or neutral. B1 also stands out with only one neutral answer, and 58.3% of answers in the "Strongly agree" category. These results imply that the experts place most importance on third-party interest in gathering information from and seeking control over personal environments (B1 and B2), and ICT developers not recognizing the need for variations in IoT development (B5), as barriers against autonomy. Furthermore, B7 and B9 have few neutral answers and a lot of agreement, though the agreeing answers are more distributed across the

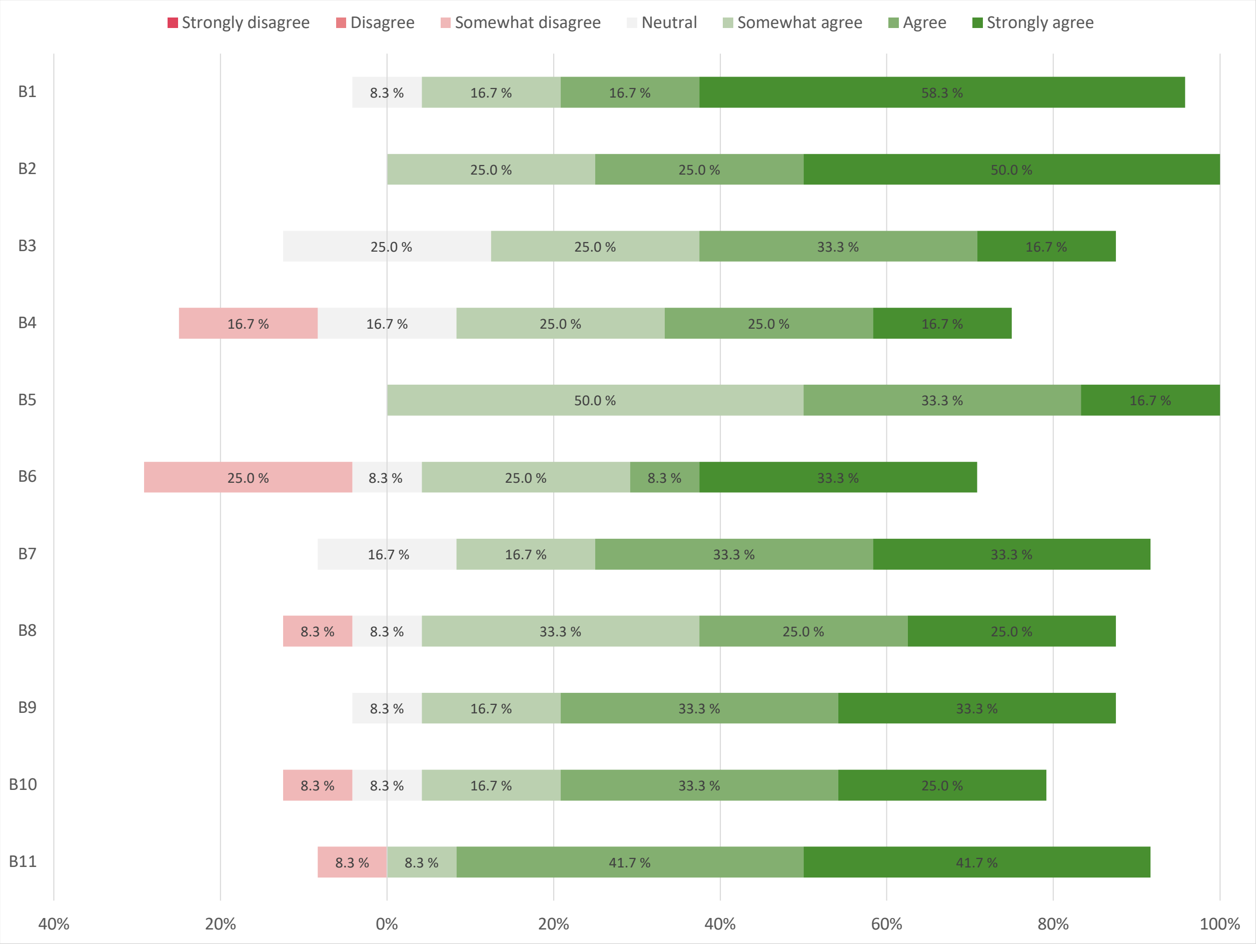


Figure 4.5: The expert panel's level of agreement to whether the presented statements are barriers towards human autonomy in IoT.

range than the aforementioned factors. This indicates that the experts place some emphasis on the speed of the evolution of IoT outpacing regulatory processes (B7), and systemic biases (B9), as barriers as well.

The statement that exhibits the most notable diversity in opinions is B6, with one-third of the responses falling into the categories of "Somewhat disagree" or "Neutral," while the remaining two-thirds fall within the agree range. This observation indicates a lack of consensus among experts concerning the extent to which dependence on centralized authorities and service providers (B6) hinders human autonomy in IoT. Additionally, B3 received the highest proportion of neutral responses, suggesting that some experts do not perceive it as having a significant impact on autonomy.

Assessing the barriers' significance for future IoT (Q3)

To provide an answer to Research Question 3 and assess the significance of the barriers for future IoT, the following scenario was presented in the survey, and the participants were asked to rate each statement according to how important it will be for achieving the scenario within 2035.

> **Scenario 2**: By 2035, smart environments and IoT will be built in a way so that humans lose agency, resulting in a loss of personal freedom, diminished privacy, and control over one's life.

The results of the assessment of the barriers are illustrated in Figure 4.6, a 100% stacked bar chart where each bar represents a barrier statement, mapped using the B1 through B11 codes to refer to Table 4.8. The chart employs the same color scale and labelling as Figure 4.3.

From Figure 4.6, it is clear that the expert panel deems B1, B2, and B10 the most important factors for achieving Scenario 2. This is reflected by their agreement levels in Figure 4.5, where these barrier statements have almost all answers on the agree range. In Figure 4.6, B3 and B7 stand out as having the most neutral answers, with one-third falling in this category. Only two of the barrier statements, B2 and B4, have an answer in the "Not at all important" category. The rest are of low importance or higher. Furthermore, statements B3, B4, B11, and to some degree B8, differs from the rest in having answers distributed throughout the importance scale, implying there is little agreement about these factors' significance for achieving Scenario 2. The average importance score of all the barriers have been calculated to compare with the end-users' scores in Section 4.3 (see Table 4.12 specifically).

Again, X10 states that the factors do not do anything in isolation, in addition to asking questions of the incentives behind the development of IoT:

> *None of these factors by themselves is contributing to this scenario, they are interlinked and intertwined. I think an important part of our responsibility as social scientists in this field is understanding how and why and to which degrees these factors are intelinked and who benefits from IoT. We might start by asking: Why do we need IoT in the first place. Are there alternative ways of imagining the future?*

On the other hand, X3 does not see B4 as a barrier, but expresses that it can be an enabler of autonomy by easing configuration:

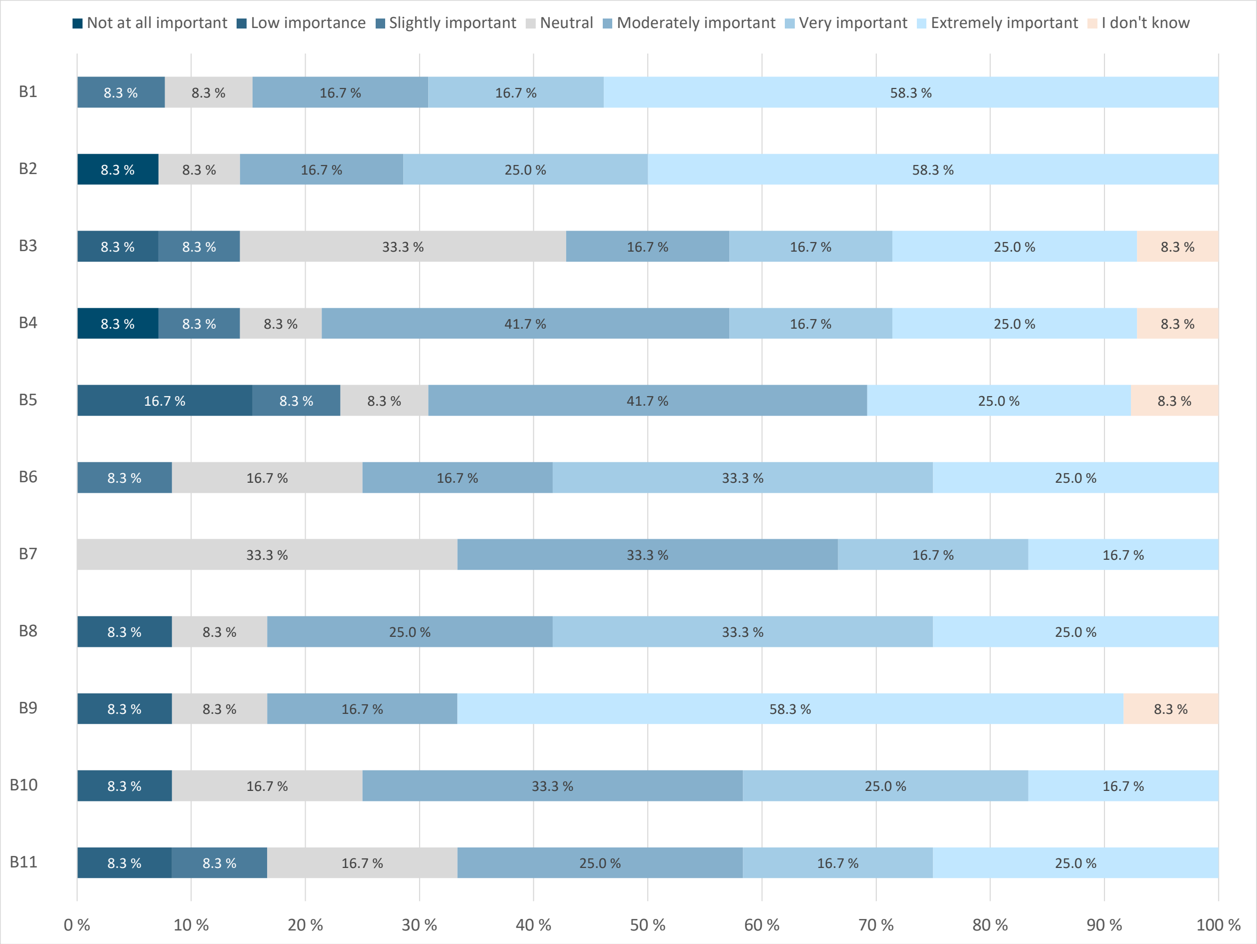
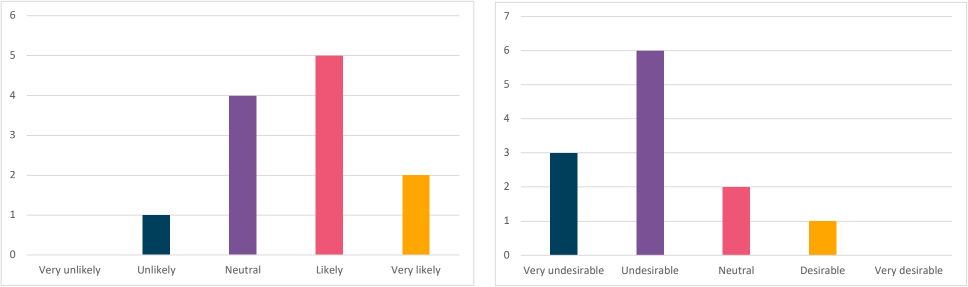


Figure 4.6: Stacked bar chart depicting the importance levels assigned by the expert panel to the presented factors for achieving Scenario 2 in the future of IoT.

> *Also, I think that centralized systems and limited options can actually *contribute* to human autonomy, because they tend to simplify the configuration problem.*

Lastly, Figure 4.7, comprised of two bar charts, summarizes the the results from asking the expert about the likelihood and desirability of Scenario 2. Figure 4.7a illustrates the experts' anticipated likelihood of Scenario 2 becoming a reality within 2035, and Figure 4.7b depicts how desirable they find it, regardless of viability. Generally, there is agreement that the scenario is undesirable yet likely. More than half of the participants believe the scenario to be likely or very likely, and one-third are neutral - implying there is a possibility that it will happen. Additionally, as many as three-fourths find it undesirable or very undesirable.



(a) Likelihood of S2.

(b) Desirability of S2

Figure 4.7: Two bar charts depicting the experts' judgement of the likelihood and desirability of Scenario 2.

4.3 Results from the End-User Survey

The objective of the end-user survey was to investigate perceptions of human autonomy, and assess the barriers and enablers identified in the literature review from the point of view of the general public, and together with the expert survey contribute towards providing an answer to (RQ1), RQ2, and RQ3. This section follows the same structure as the one above. First, a general description of the sample is given. Second, the participants' definitions of human autonomy are presented in the form of two bar charts, as well as direct quotes from the survey. Thirdly, the results from the evaluations of enablers from the literature are presented, accompanied with any new factors as identified by the end-users. Lastly, the same is done for the assessment and identification of barriers.

4.3.1 Sample Description

This section describes the sample in the end-user survey, which consists of a total of 123 participants. The participants' age, gender, geography, level of education, occupation, and attitude towards new technology are the characteristics that will be presented through charts and text descriptions. Figure 4.8 is a bar chart portraying the age and gender distribution of the sample. From Figure 4.8 it is evident that the largest subgroup is females between the ages 18-34, comprising 50.4% of the total sample. Overall, two-thirds of the participants identify as women, while most of the

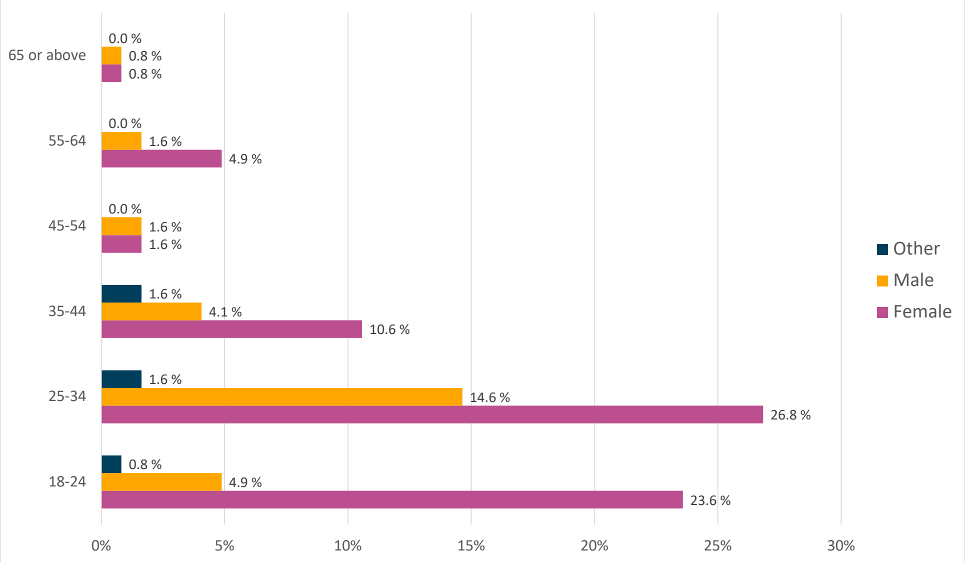
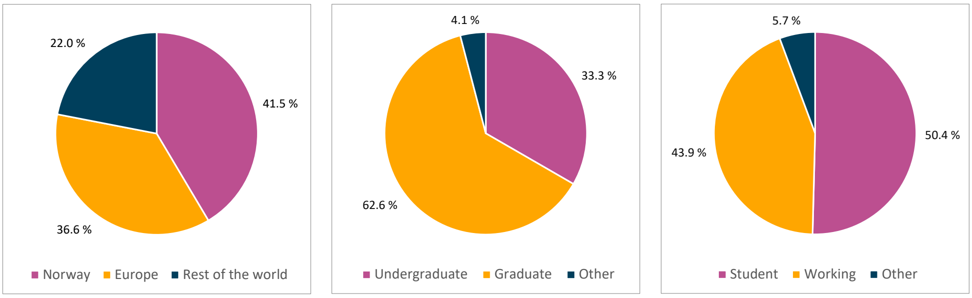


Figure 4.8: The gender and age distribution among participants in the end-user survey.

rest identify as men, and some fall into the categories of either non-binary, other, or chose the "prefer not to say" option.

Figure 4.9 combines three pie charts to give an overview of the geography, education, and occupation of the participants. From Figure 4.9a, it can be observed that around 40% of the participants have their permanent residence in Norway, one-third are are from other parts of Europe, and the last 22% are located outside of Europe. The participants who fall into the "rest of the world" category are distributed across North America, Africa, Asia, Australia, and a few chose "Other". Figure 4.9b describes the level of education of the participants, and implies that the sample is generally highly educated. The "Undergraduate" category combines those who answered that they have a bachelor's degree (30.1%) with upper secondary school (3.3%), whereas the "Graduate" category combines master's degree (56.1%) and doctorate/Ph.D. (6.5%). Lastly, Figure 4.9c, depicts the participants' occupations. Around half of the sample consists of students, 43% are working, and the last 4.1% are either unemployed/job seekers, unable to work, or retired.



(a) Geography **(b)** Education **(c)** Occupation

Figure 4.9: Three pie charts depicting the end-users' geography, level of education, and occupation.

The last segment in the demographic description is the end-users' attitude towards new technology. Figure 4.10 is a diverging stacked bar chart showing the results from the participants' level of agreement to the three technology statements they were presented with. When asked if they follow emerging technologies and trends relate to IoT, AI, or smart systems, 54.5% of participants place themselves on the agree range. Not as many consider themselves early adopters of new technology, but around one-third do. Finally, most of the respondents are positive to new technology, only 29.3% of participants to some degree regard themselves as especially sceptical towards new technology. Altogether, Figure 4.10 suggests that the sample is predominantly interested in new technology and not too sceptical, but they are not necessarily the first to adopt new products.

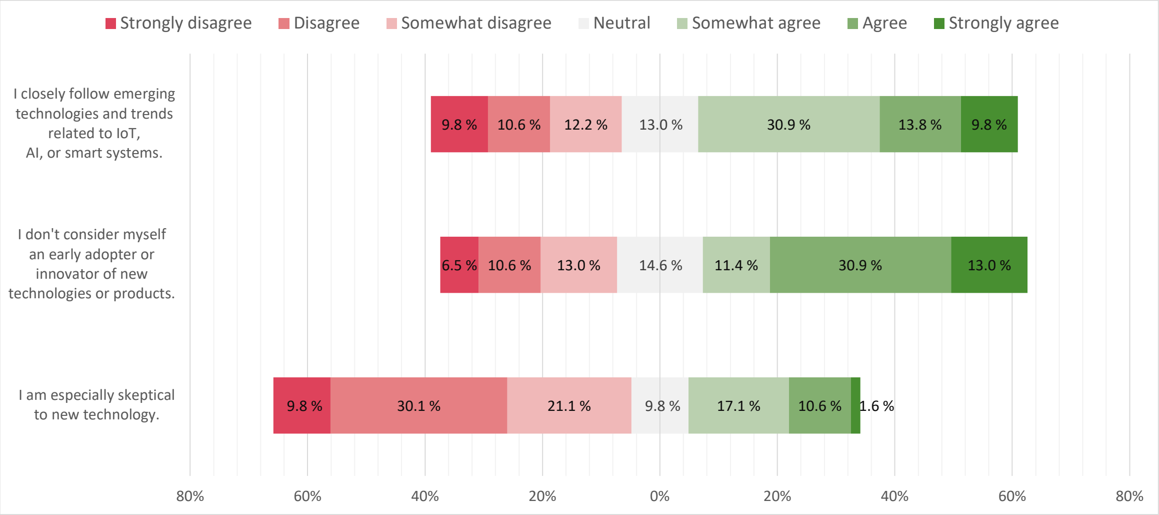


Figure 4.10: The end-users' attitude towards IoT and emerging technologies.

4.3.2 Autonomy

This next section highlights how the end-users' interpret human autonomy in an everyday-life context, and in an IoT context. Figure 4.11 is a bar chart depicting the users' impression of human autonomy in their everyday life. As mentioned, the definitions of autonomy can be categorized as political, moral, and personal autonomy, corresponding to the codes D1, D2, and D3, in the chart, respectively. From the figure it can be observed that the majority of the end-users place importance on not being restricted by others or technology, i.e., political autonomy, in their definition of the term. Four of the participants picked "Other", and were asked to define the term in their own words. Two described autonomy as a combination of the definitions listed as D1 and D2. The third participant wrote "It means different varied things, including: My ability to do things freely without technology or to work autonomously.". The last definition differs from the rest, touching upon D1, but from a perspective that questions the nature of freedom and autonomy:

> *A balance, I guess. There are rules (from "wear seatbelt" to "solitary confinement because of virus") that apply. Freedom is to just adapt to that and have your mind believe this is what you wanted all along.*

When asked to define human autonomy in an IoT context, the majority was concerned with controlling the system and the data they share with it. See the bar chart in Figure 4.12 for the distribution of answers. The chart includes the same definitions as previously, but they are modified slightly to better be suitable for the

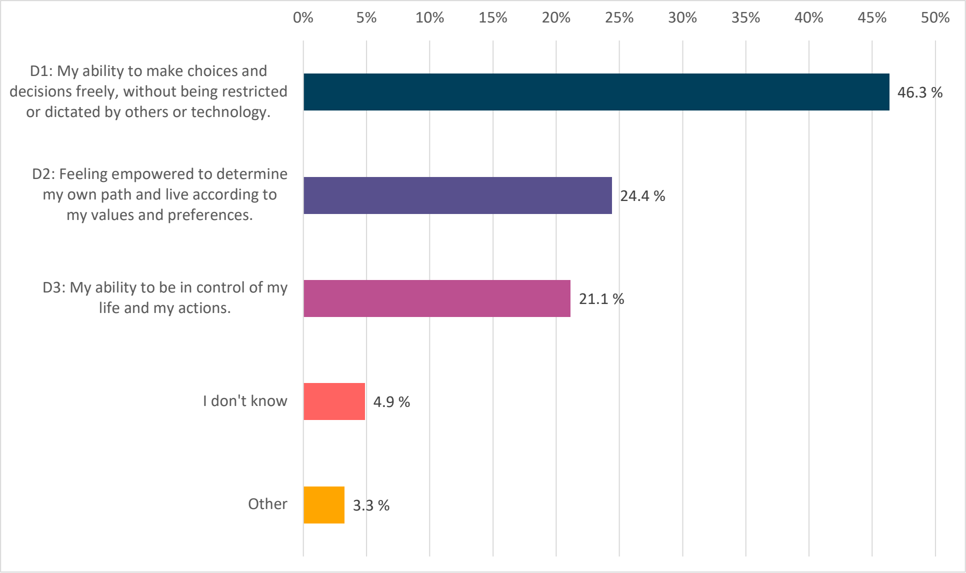


Figure 4.11: The end-users' definition of human autonomy in an everyday-life context.

question about the IoT context, and are therefore listed as D1*, D2*, and D3*. Only one participant chose the "Other" option for this question, and their answer is a combination of D1* and D3*:

> *My ability to control the system and the information I share with it, free of any implicit or explicit influence from the restrictions and biases of those technologies.*

This is the same participant who defined autonomy as a combination of D1 and D2 in the previous question. Another point that is noteworthy from the results, is that that around half of the participants who picked D1 in the previous question, selected D3* in this question.

Lastly, the definitions differ between experts and end-users. Figure 4.13 is a bar chart comparing the categorization of definitions of autonomy between experts and end-users. From the figure is clear that the majority of the experts place emphasis on personal autonomy, whereas the end-users are more concerned with political autonomy.

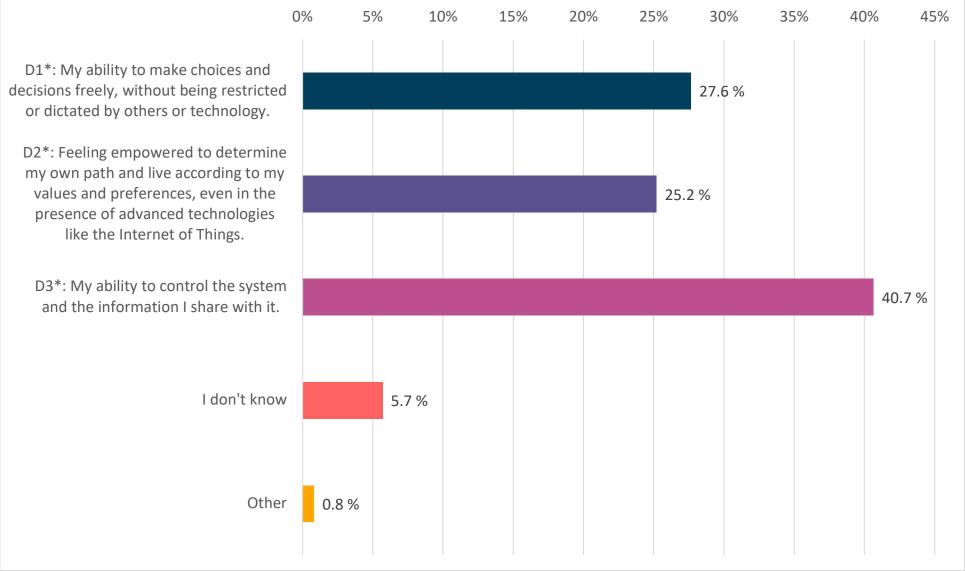


Figure 4.12: The end-users' definition of human autonomy in an IoT context.

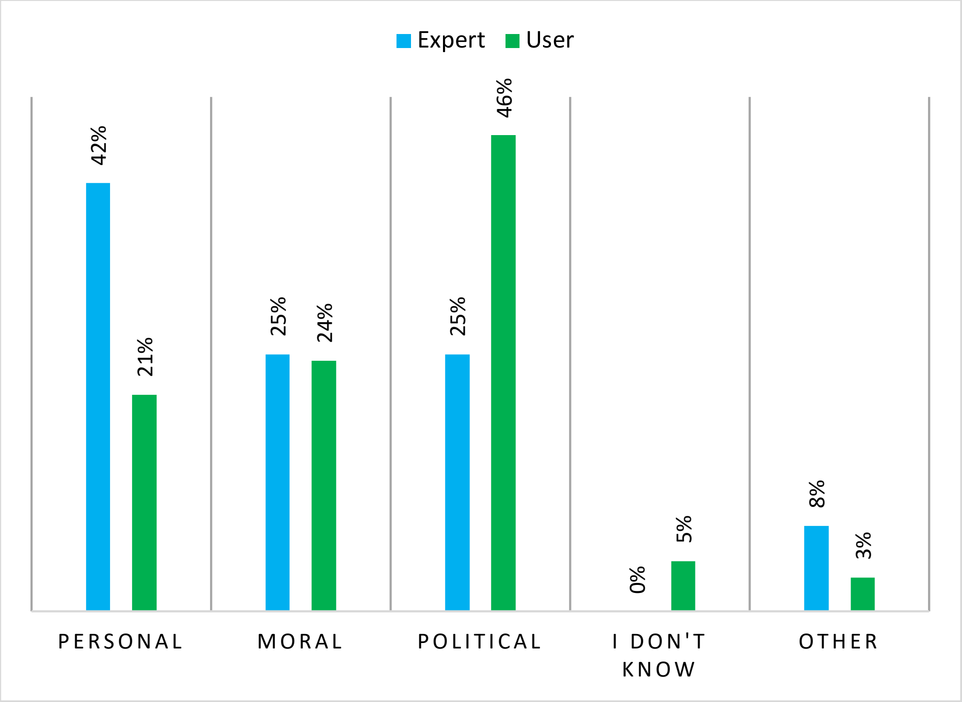


Figure 4.13: Expert versus user perspective on the definition of autonomy.

4.3.3 Enablers

The next section presents the results from section 4 of the end-user survey, see Appendix F for the specific questions that were asked. First is the quantitative data from the rating of enabler statements, followed by the qualitative data from the open-ended question about which enablers are most important, and lastly the rating of the enablers' importance for future IoT.

To create the statements to be used in the end-user survey, the phrasing of the enabler statements from the expert survey (see Table 4.7) was modified to make it more comprehensible for those with less technical knowledge. Table 4.9 lists these statements as they were worded when presented to the participants in the end-user survey.

Figure 4.14 is a diverging stacked bar chart, illustrating the end-users' level of agreement to whether the presented statements describe mechanisms that enable human autonomy in today's IoT. The statements are mapped using a capital E (for enabler) and a number between 1 and 11 (i.e., E1, E2, etc.), where the codes refer to the statements in Table 4.9. The chart employs the same color scheme and labelling as the figures in Section 4.2. The "I don't know" answer option is omitted from the chart to make it more comprehensible. For reference, the percentage of participants who said "I don't know" was less than 9% for all statements.

Overall, Figure 4.14 shows that the end-users' answers are predominantly in the agree range, which means that they agree that all the presented statements enable human autonomy in IoT. The high scores makes it difficult to differentiate the answers and uncover things that stick out. Four statements have a percentage over 50% that strongly agree, namely E3, E6, E7, and E10. This means that the end-users concur that openness about collection, processing, and use of data in IoT (E3), regulatory frameworks such as GDPR (E6), ethical design principles for the development of IoT (E7), and information and communication security (E10) enable autonomy. Yet, there are a few of the enablers that have less agreement. E1, E2, and E9 are the statements with the highest degree of disagreement, and E9 also has the highest percentage of neutral answers and lowest percentage of "Strongly agree". This indicates that the end-users place less emphasis on end-user customization of machine-to-machine (M2M) communication (E1) and personalized privacy suggestions from the IoT system (E2) as enablers, and that some believe that new ways for H2M communication (B9) does not impact autonomy to a large extent. Compared to the experts, the end-users generally have more faith in the presented statements as enablers.

The participants were then given an optional open-ended question about which enablers they believe to be most important for human autonomy in future IoT. Here,

Table 4.9: Enabler statements presented to the participants in the end-user survey.

Code	**Statement**
E1	Letting people adapt to their specific needs how smart devices (i.e., smart watch and mobile phone) interact with each other in a way that doesn't require technical expertise.
E2	Providing personalized suggestions on how to keep information private when sharing and using data with smart devices connected to the Internet of Things.
E3	Making sure that smart devices are open and clear about how they collect, process, and use your information, so users can understand what happens with their data.
E4	Accessibility to smart devices for users with impairments, such a configurable user interface that can be adjusted according to the levels of a user's abilities.
E5	Designing privacy policies (i.e., at specific device or service level) that are easy to understand.
E6	Regulations and legal frameworks (i.e., GDPR) that have implications for which types of personal data can be gathered about users, how the data can be used, etc.
E7	Principles for developing IoT systems in an ethical and responsible way, i.e., IoT developers considering and prioritizing privacy and ethics from the beginning of development.
E8	The system sends messages or notifications to warn users when they might be sharing personal data that could be risky, i.e., an alert that pops up when the user is about to share sensitive data.
E9	Offering new and creative ways for people to communicate with machines, such as using voice commands or easy-to-use interfaces when interacting with smart devices.
E10	Improving the protection of information and making sure that communication networks are secure from potential threats or unauthorized access.
E11	Ensuring that responsibility is clearly assigned and understood among different parties in complex IoT systems and networks of interconnected systems.

a lot of the abovementioned enablers (see Table 4.9) were referred to, including the following: simplicity, transparency, accessibility, accountability, security and privacy, designing for the users' needs and not monetization, regulatory frameworks, customization and configurability of services, H2M interaction features and interfaces, alerts about security risks and breaches. Being able to control a smart home

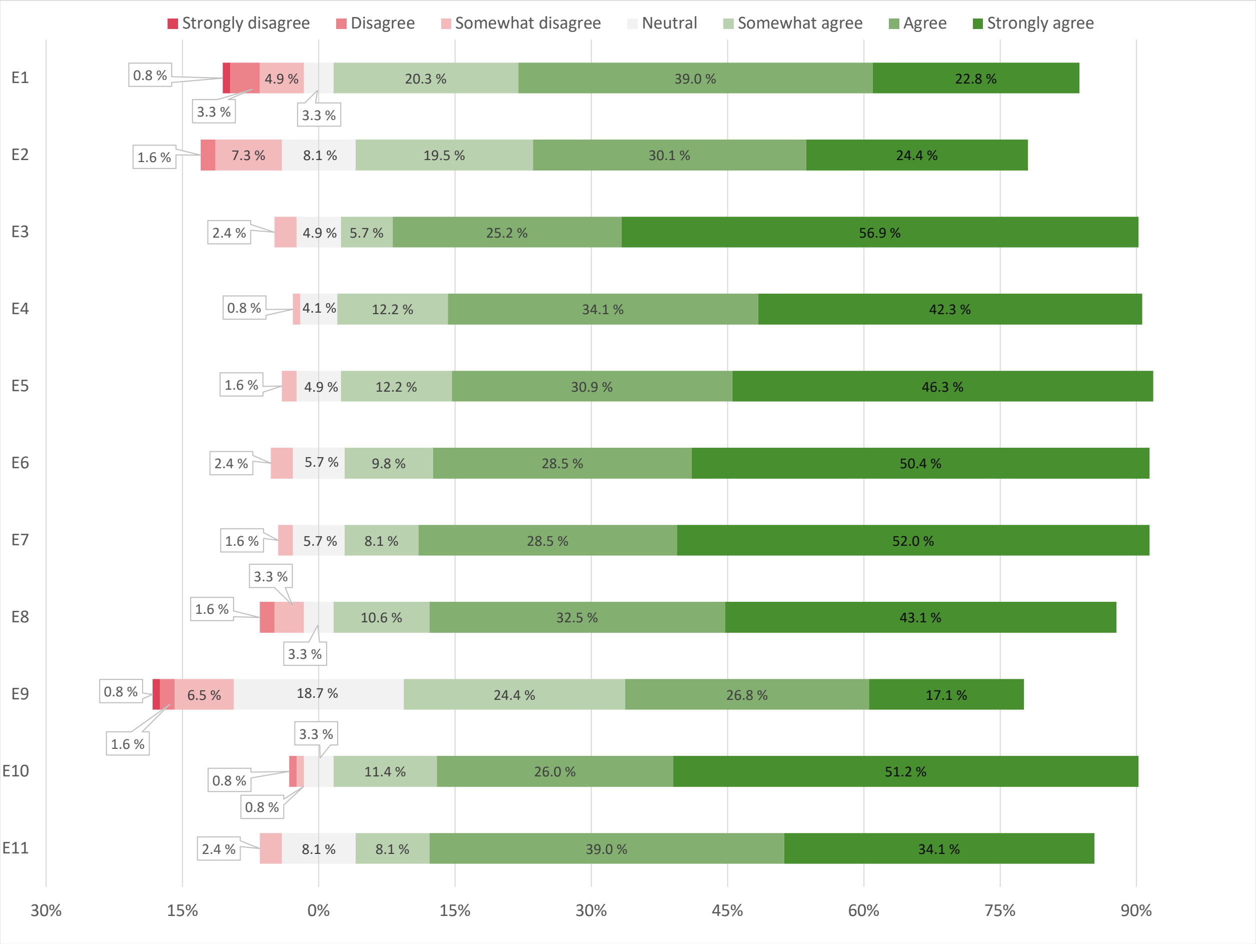


Figure 4.14: The end-users' level of agreement to whether the presented statements are enablers of human autonomy in IoT.

environment via a user-controlled hub was also brought up, this exact technical implementation was also found in the literature [JKH20]. Another technical mechanism related to privacy that was remarked was having to turn on sharing abilities if desired and having them turned off as default.

One factor that was mentioned several times by the end-users, that was identified in the literature but not included in the survey, was education. Both ensuring that the public is aware of the consequences of use, that they understand why technologies have been implemented, and they are made aware of their rights were aspects brought up. In relation to this, an interesting point was made about the education of developers and ethics. As one participant stated about university education:

> *We need to make sure that universities are training engineers who are technically competent to design the technology correctly (for example, without security vulnerabilities and with good user interfaces) and with a strong sense of ethics (for example, refusing to design systems that spy on users).*

Lastly, the end-users also came up with two factors that were not identified in the literature review. One is the ability to opt out of IoT entirely:

> *I think [..] it is essential that people have the ability to opt out of such technologies. There is a risk that if societies as a whole become increasingly dependent on people using IoT technologies (e.g., smart meters being used by energy companies to determine an individual's tariff) then increasingly individuals who cannot or do not wish to use the technology, for whatever reason, may have more fundamental rights undermined (e.g., the right to housing, the right to heat their home). Regulatory innovations must work to always include those who do not wish to adopt, and avoid putting in place regulation that simply assumes everyone will wish to adopt these technologies.*

Related to paternalistic behaviour of the technology, one of the participants called for a way to control how much personlization is enabled:

> *The main aspect of technology that limits user autonomy is the tendency of technology to try to adapt entirely to users' existing preferences. Eventually, this means that users end up in a virtual environment that matches exactly all their habits, beliefs, and perceptions, and this gradually removes the freedom of the user to make NEW choices, consider NEW possibilities, or change in any way. In this sense, technology removes autonomy by detaching users from reality [...] there should be an option for people to control how much personalisation/learning is enabled in the technologies they use.*

Assessing the enablers' significance for future IoT (Q3)

To provide an answer to Research Question 3 and assess the significance of the enablers for future IoT, the end-users were presented with the same **Scenario 1** as the experts, and asked to rate each statement according to how important it will be for achieving the scenario within 2035.

The results of the end-users' assessment of the enablers are illustrated in Figure 4.15, a 100% stacked bar chart where each bar represents an enabler statement, mapped using the E1 through E11 codes to refer to Table 4.9. The chart employs the same color scale and labelling as the equivalent figures in Section 4.2.

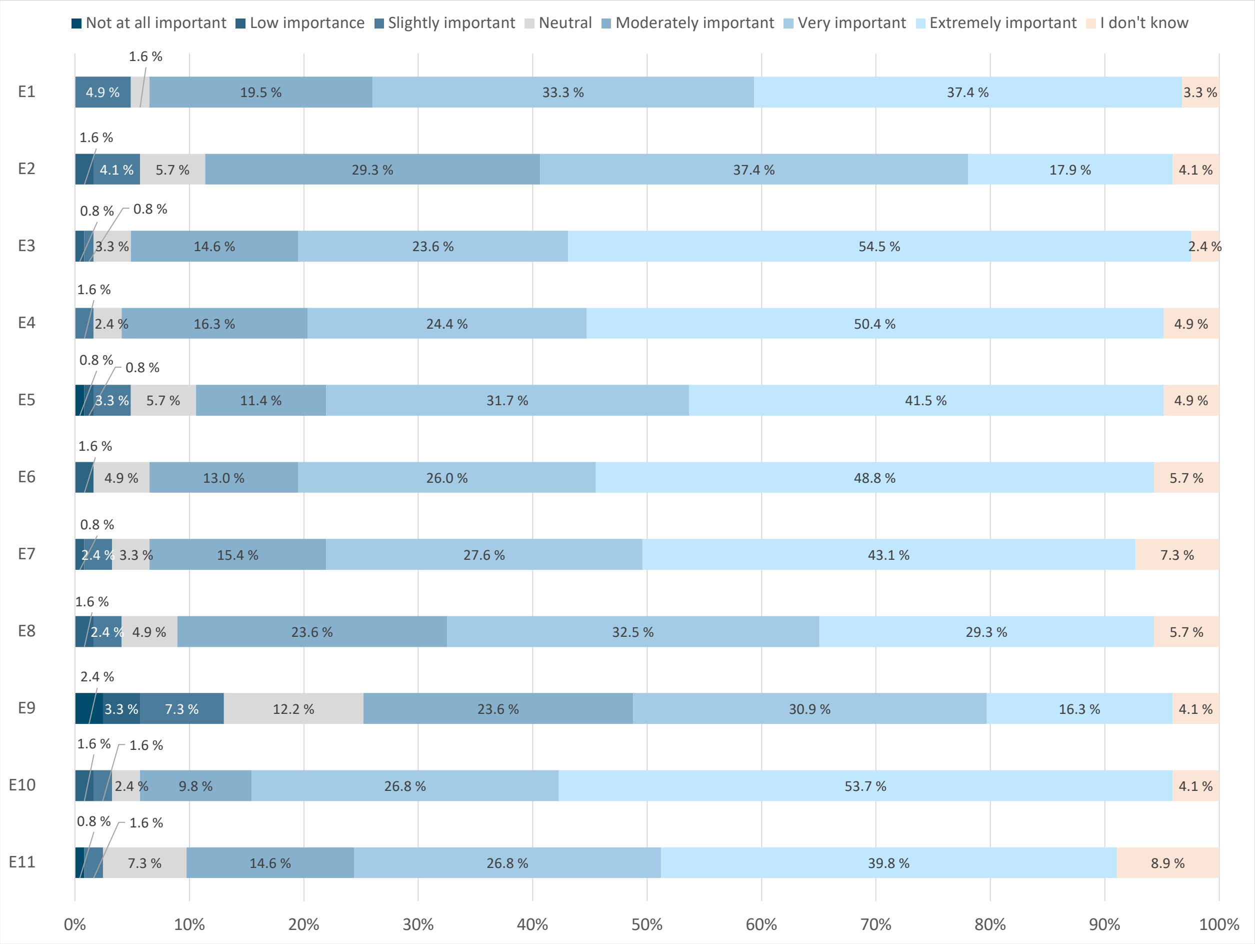


Figure 4.15: Stacked bar chart depicting the importance levels assigned by the end-users to the presented enablers for achieving Scenario 1 in the future of IoT.

From Figure 4.15, it is clear that the end-users deem the majority of enablers very important for achieving Scenario 1. Only two statements, namely E2 and E9, have a percentage of answers that is lower than 29% in the "Extremely important" category. E9 is the enabler that is deemed least important for ensuring autonomy in future IoT. It also has most distribution of answers, and is the statement most are neutral towards, with 12.2% in this category.

The average importance scores have been calculated and can be viewed in Table 4.10. The table lists the enabler statements E1 through E11 along with the average scores and their standard deviation, of end-users and experts for comparison. The "I don't know" answers have been omitted from the calculation to get an even scale, ranging from 1 (least important), to 7 (most important). The "Mean diff" column displays the difference between average scores by subtracting the expert score from the user score.

Table 4.10: A comparison between end-users and experts: the average importance score of enabler statements for achieving Scenario 1.

Code	Expert mean	σ_E	User mean	σ_U	Mean diff
E1	5.1	1.1	6.0	1.1	+0.9
E2	4.9	1.2	5.6	1.1	+0.7
E3	5.9	1.3	6.3	1.0	+0.4
E4	6.1	1.2	6.3	0.9	+0.2
E5	5.8	1.4	6.0	1.2	+0.2
E6	5.4	1.3	6.2	1.1	+0.8
E7	5.9	1.4	6.1	1.1	+0.2
E8	4.6	1.2	5.8	1.1	+1.2
E9	5.2	1.3	5.2	1.5	0.0
E10	5.5	1.5	6.3	1.1	+0.8
E11	5.3	1.4	6.0	1.1	+0.7

From Table 4.10, it becomes clear that the end-users have more faith in the enablers than the experts for for achieving Scenario 1, since the average scores are higher for absolutely all the enablers.

4.3.4 Barriers

The next section presents the results from part 5 of the end-user survey, see Appendix F for the specific questions that were asked. First is the quantitative data from the rating of barrier statements, followed by the qualitative data from the open-ended question about which barriers are most important to address, and lastly the rating of the barriers' importance for future IoT.

To create the statements that were utilized in the end-user survey, the phrasing of the statements from the expert survey (see Table 4.8) was modified to make it more comprehensible for those with less technical knowledge. Table 4.11 lists these statements as they were worded when presented to the participants in the end-user survey.

Table 4.11: Barrier statements presented to the participants in the end-user survey.

Code	**Statement**
B1	Third-party interest in gathering information from personal intelligent environments (surveillance).
B2	Third-party interest in seeking control over personal environments.
B3	User configuration capabilities and settings in smart devices being hidden or hard to find.
B4	Smart devices limiting the user's control options to specific pathways programmed by the developers.
B5	ICT developers not recognizing the need for variations in development of smart devices.
B6	Dependence on a few powerful organizations or companies that control important services and data, which can result in a situation where they have a lot of control over IoT user information, like a monopoly.
B7	The Internet of Things (IoT) is developing very quickly, but the rules and regulations to govern it are not keeping up, possibly making it harder for regulations to work well and do their job effectively.
B8	Limited support for ensuring informed consent in IoT, i.e., giving users the opportunity to accept or oppose data collection and use.
B9	Systemic biases/unfairness existing within how services are provided. I.e., biases in how businesses operate, compete in the market, or how regulations are set up.
B10	Users may not have all the information they need to understand what might happen when they share their data, i.e., when systems collect information about their location.
B11	The Digital Divide – unequal access to technology (such as IoT) in society, potentially disadvantaging part of the population.

Figure 4.16 is a diverging stacked bar chart, illustrating the end-users' level of agreement to whether the presented statements describe mechanisms that inhibit human autonomy in today's IoT. The statements are mapped using a capital B (for barrier) and a number between 1 and 11 (i.e., B1, B2, etc.), where the codes refer to the statements in Table 4.11. The chart employs the same color scheme and labelling as the figures in Section 4.2. The "I don't know" answer option is omitted from the chart to make it more comprehensible. For reference, the percentage of participants who said "I don't know" is less than 8.2% for all statements, except from in B5 and

B9 where 13% chose this option.

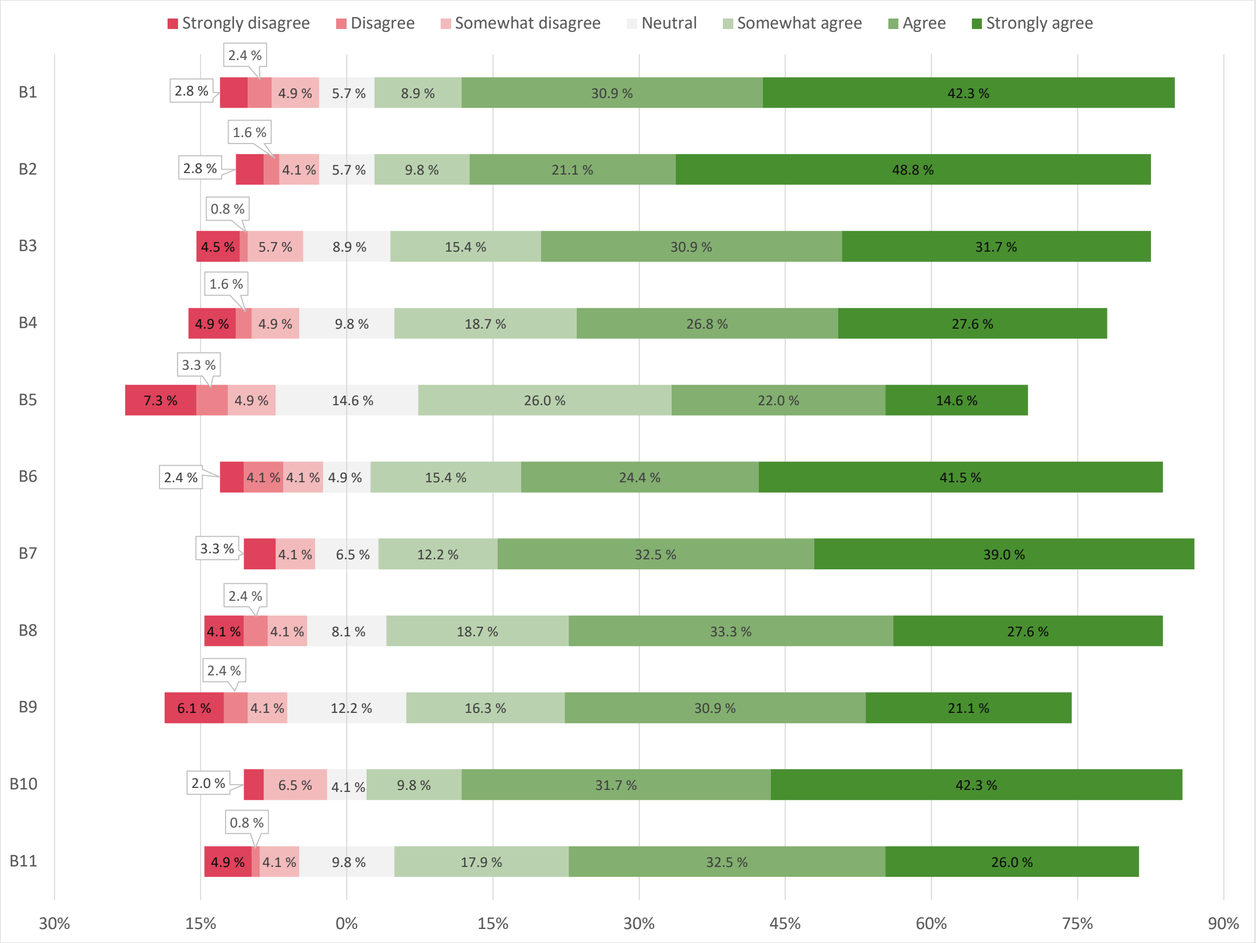


Figure 4.16: The end-users' level of agreement to whether the presented statements are barriers towards human autonomy in IoT.

From Figure 4.16 it can be observed that B1, B2, B6, and B10 have the highest percentages of answers within the "Strongly agree" option. This implies that the end-users believe third-party interest gathering information from and seeking control over personal environments (B1 and B2), monopoly-tendencies (B6), and the fact that users may not have all the information they need to understand what happens when they share their data (B10), to be the most significant barriers to autonomy in today's IoT. As mentioned in the previous paragraph, B5 and B9, have the highest percentages of participants saying "I don't know". These are also the statement where the answers are most distributed over the entire range, and the statements with the highest percentages of disagreement and neutrality. This means that the end-users don't agree whether ICT developers not recognizing the need for variations in IoT development (B5), and systemic biases within how IoT services are provided (B9), are barriers to autonomy. Compared to the experts, this is the opposite: the experts had higher consensus about these statements as barriers. However, it must be noted that B5 and B9 still have the majority of answers on the agree range.

Generally speaking, as indicated by the distribution of answers in Figure 4.16, there is more disagreement among the end-users about the barriers to autonomy than there is about the enablers. Compared to the experts, this is the opposite: the end-users agree most about the enablers, while the experts agree most about the barriers. This indicates that end-users have more faith in the enablers than the experts, and that the experts find the barriers to be more exigent than the end-users do.

The participants were then given an optional open-ended question about which major challenges they believe need to be addressed to ensure human control and decision-making power in the IoT ecosystem. Here, a lot of the abovementioned barriers (see Table 4.11) and factors from the literature were referred to, including the following: monopoly tendencies, social biases in the technology and its development, too much and complicated information making it difficult for users to understand what they are agreeing to, the Digital Divide, third-party (both government and business) interest in surveillance and controlling data, slow regulation, and monetization incentives for development instead of societal benefits as incentives.

Surveillance and control of data were mentioned several times, and came across as important barriers to the end-users. Several participants proclaimed that corporate interest will always be incompatible with human autonomy. Another stated that surveillance is going to happen regardless, if it is possible within the technology:

> *If it is physical possible to track and monitor someone, it WILL happen, regardless of the official channels and regardless of regulations. For a corporation, any fine for privacy breaches will just be racked up to "cost of doing business". For a government, they will not tell you they are monitoring you, but if your choices to not match their program you WILL be punished for it. The urge to control others is very strong in human nature. We simply cannot allow any paths for that to happen. I have no "smart" devices now and have no plans to ever buy any. I am perfectly capable of managing my home without them.*

Another factor that several of the end-users stressed, was regulation and legal frameworks to mitigate money-driven incentives of businesses. One participant gave the following declaration, which also provides some insight into their belief that adequate regulation is unlikely to be put in place in the future:

> *There is an urgent need for regulation - companies that operate black box technologies (such as machine learning) cannot be trusted to self-regulate in the interests of individual consumers, especially when those companies rely on consumers to harvest big data for use in re-selling or in analytics. Companies incentivised to continually harvest data from its users will create systems that keep users 'hooked' in some way, either by increasing reliance on the technology or obscuring the ways in which data is obtained. In order to regulate effectively, analytical and inferential techniques must be open to public regulatory scrutiny. This is unlikely to happen due to competition between corporations and the protection of trade secrets.*

Lastly, an interesting statement was made by one of the respondents, who seems to believe that unequal access to technology is not a barrier but an enabler of autonomy:

> *[..] inequality I think will not be a barrier. It never was, and rather is an enabler, as it gives the people who are able to participate another way of setting themselves apart from the mass. Thats unfortunte, but thats how societies still work.*

Assessing the barriers' significance for future IoT (Q3)

To provide an answer to Research Question 3 and assess the significance of the barriers for future IoT, the end-users were presented with the same **Scenario 2** as the experts, and asked to rate each statement according to how important it will be for achieving the scenario within 2035.

The results of the end-users' assessment of the barriers are illustrated in Figure 4.17, a 100% stacked bar chart where each bar represents a barrier statement, mapped using the B1 through B11 codes to refer to Table 4.11. The chart employs the same color scale and labelling as the equivalent figures in Section 4.2.

From Figure 4.17, it is clear that the end-users deem B1, B2, B6 and B7 the most important for achieving Scenario 2 (B8 and B10 are not far behind, but B8 has some neutrality as well), although it is difficult to differentiate when all ratings are quite high. B5 and B9 stand out as the barriers with most dispersion in answers. B5, B9, and B10 stand out with more dispersion in the answers, and a higher percentage who replied with "I don't know", B9 having the highest amount with 13.8% in this category.

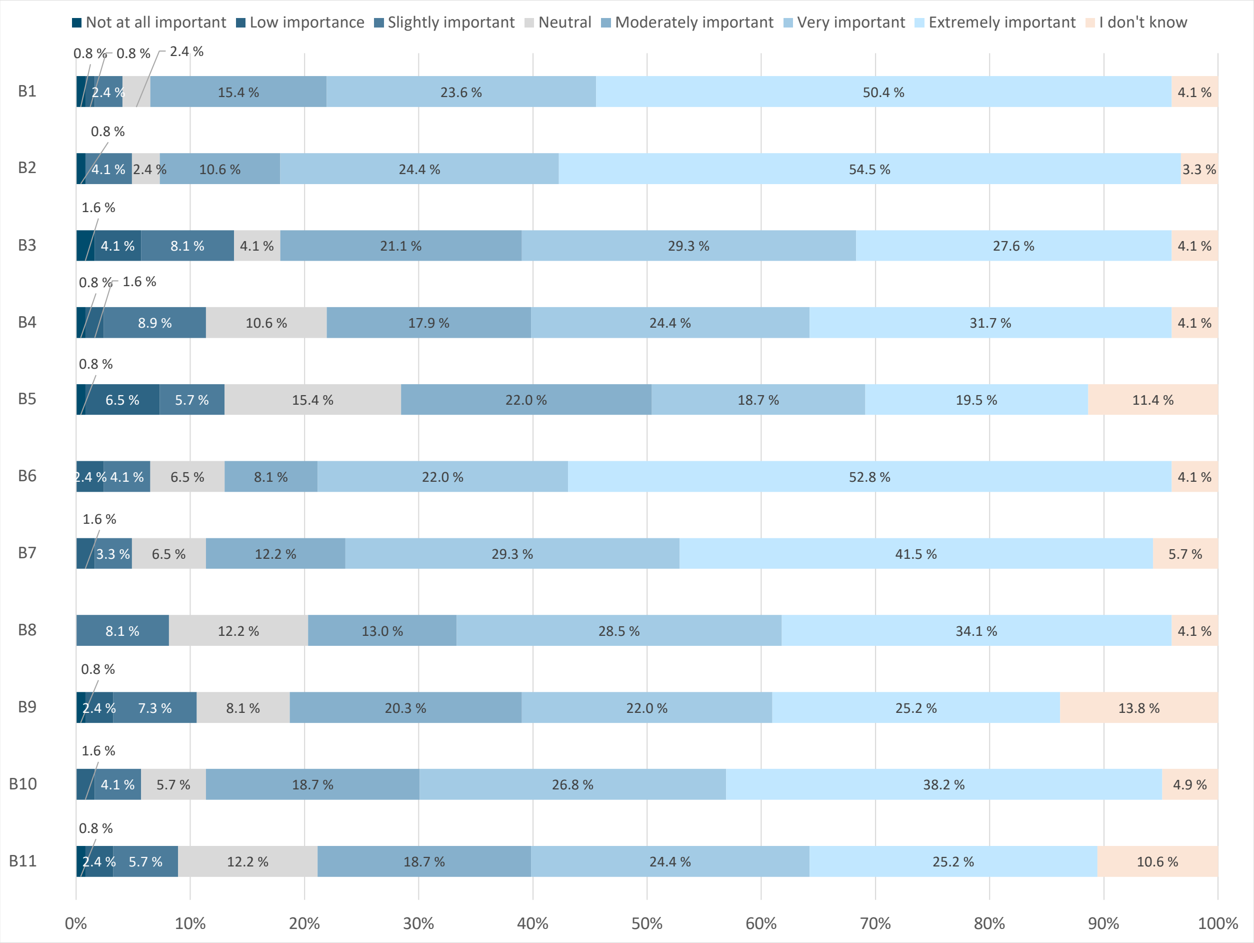


Figure 4.17: The end-users deemed importance level of barriers for achieving Scenario 2 in future IoT.

The average importance scores have been calculated and can be viewed in Table 4.12. The table lists the barrier statements B1 through B11 along with the average scores and their standard deviation, of end-users and experts for comparison. The "I don't know" answers have been omitted from the calculation to get an even scale, ranging from 1 (least important), to 7 (most important). The "Mean diff" column displays the difference between scores by subtracting the expert score from the user score.

From Table 4.12, it appears that the experts and end-users agree about the significance of B1 through B5 and B8 for achieving Scenario 2, since the difference between the scores are less than or equal to 0.2. The only barrier the experts gave

Table 4.12: A comparison between end-users and experts: the average importance score of barrier statements for achieving Scenario 2.

Code	**Expert mean**	σ_E	**User mean**	σ_U	**Mean diff**
B1	6.3	1.1	6.2	1.2	-0.1
B2	6.3	1.1	6.2	1.1	-0.1
B3	5.3	1.4	5.5	1.5	+0.2
B4	5.5	1.3	5.5	1.4	0.0
B5	5.0	1.6	5.1	1.5	+0.1
B6	5.5	1.3	6.1	1.3	+0.7
B7	5.2	1.1	6.0	1.2	+0.8
B8	5.8	1.4	5.7	1.3	-0.1
B9	5.9	1.7	5.5	1.4	-0.4
B10	5.2	1.4	5.9	1.2	+0.7
B11	5.1	1.6	5.5	1.4	+0.4

notably higher score than the end-users did, is B9. Generally, the end-users rated all the other barriers as important or more than the experts, but B6, B7, and B10 have the greatest differences.

Feedback From Participants

Although some participants in the end-user survey found the questionnaire somewhat difficult to follow, some also expressed their view that the chosen topic was intriguing and relevant. This positive response highlights the importance of the research area and underscores the participants' engagement in the study.

Chapter 5 Discussion

The first key objective of this thesis has been to investigate the different definitions of human autonomy and how these can be technically translated into intelligent environments and the IoT. Moreover, the thesis has attempted to state the main technical and non-technical factors that can be enablers and barriers of human autonomy in the IoT, and assess their importance for the future. For this purpose, a systematic literature review and two surveys were conducted. The research produced insights into interpretations of autonomy and a set of factors with data on their perceived importance according to a panel of twelve experts and a sample of 123 end-users.

The aim of this chapter is to interpret the findings and analyze the results to provide answers to the research questions, and explore further implications the results may have. The results of the surveys imply that there exist aspects of human autonomy that are important to end-users, which have not been considered in the development of human-centric IoT. Firstly, issues relating to the mapping of factors and categorization of barriers of enablers are discussed. Secondly is the consideration of different definitions of autonomy and how to take them into account in the IoT ecosystem. Then follows a discussion of the scenarios and implications of enablers and barriers for future IoT. Lastly, this chapter ends with a review of the results' general validity.

5.1 Mapping of Factors from the Literature

A first observation based on the findings is that the distinction between enablers and barriers to human autonomy can be context-dependent and subjective. To exemplify, how each factor is enabling or inhibiting depends on the perspective and the specific circumstances. As such, during the work of going through the literature and mapping the main factors that influence human autonomy in IoT, it became clear that it can be difficult to categorize a portion of the factors as either barriers or enablers.

Some are naturally two sides of the same coin: more of it can enable autonomy, and less of it can inhibit autonomy. Take for instance transparency. The results of the literature review and both surveys strongly suggest that implementing more transparency in IoT devices would promote human autonomy, and based on that the factor can be categorized as an enabler. On the other side, one could argue that there currently is little transparency in IoT devices on how they operate, and how they collect and use data. This qualifies "too little transparency" to be categorized as a barrier against autonomy. Evidently, these are two aspects of the same issue, which can vary depending on the perspective and context they are viewed from.

Secondly, sometimes the issue can be more complex. Many of the factors are interrelated, either directly or indirectly, and in the system they may influence each other. For example, limited support for transparency in IoT devices can be a barrier. This is clearly related to transparency, but simultaneously has to do with HCI and interfaces for how to best communicate the information to the user. This again can relate to having good enough tools for building software and hardware that are intuitive to the user, and express to the user in a clear way how they function. Thus, it is easy to state that implementing more transparency would enable autonomy, but difficult to determine how this should be done practically.

However, some factors come across as distinct barriers or enablers. Take for instance surveillance and competence/education, respectively. Surveillance is harmful to society in several ways. It can chill the exercise of civil liberties [Ric13], meaning that when people are aware that they are under surveillance, they will self-censor their actions, speech, and behavior. This chilling effect may have restrictive implications in society for the free flow of ideas [Ric13]. It also creates an imbalance in power between the watcher and the watched, which can lead to discrimination [Ric13] among other things. On the other hand, education has a number of benefits for society. It empowers people, improves the economy, promotes equality, and more [Dr 20]. The reason why these factors are so straightforward to categorize could be that they are commonly known as either beneficial for humanity and society such as education, or harmful to humanity and society such as surveillance. This suggests that there could be more agreement on the distinctly categorized factors, and possibly more disagreement about the two-sided factors. It will therefore be important to have a good representation of the of diverse and multi-stakeholder perspectives when considering how to address the factors technically.

The idea with mapping enablers and barriers was to try and evaluate the existing technical and non-technical mechanisms to find out what has not been considered, and what should be prioritized when attempting to build future human-centric IoT systems that protect human autonomy, empowerment, and control. In previous literature, there has been a lot of focus on the technology, its abilities and what it can do, instead of how it can be built to serve humans and humanity. As it turns out, the consequences of undermining of human autonomy and the barriers that were identified have not been taken into account in the literature when operationalizing new IoT solutions.

5.1.1 Existing factors that can be Enablers

The factors that are current enablers represent influences that preserve the protection of human autonomy, agency, empowerment, and/or control, and factors that are associated with technological developments that benefit both humans and society. The majority of enablers found in the literature were assessed by the experts as less contributing to autonomy. In addition, the list of enablers presented in the expert survey (see Table 4.7) was deemed non-comprehensive. For instance, democratic involvement of citizens in the development and use of IoT, and adjusted incentives based on humane goals and values, were gaps identified in the expert study that were not found in the literature. On the end-user side, education of developers in ethical design of technology, being able to control how much personalization the system is providing, and the ability to opt out of the IoT were mentioned. Both the experts and end-users brought up education of the public, which was identified in the literature but not included in the surveys. Moreover, the results of the statement ratings imply that end-users have more faith than experts in the enablers as preserving forces of autonomy.

When it comes to the specific enabler statements and the level of agreement to which they are enabling of autonomy, the experts were most concerned with transparency and accessibility (see Figure 4.2), whereas the users ranked these two factors high along with simple privacy policies, regulations, ethical design principles, notifications from the system about risks, and security (see Figure 4.14. This implies that the users may have more trust than the experts that the majority of the enablers also effectively preserve autonomy. The results show dispute among the experts as to whether security is an enabler, but end-users place emphasis on this. Factors that experts were more neutral towards and end-users less agreeing to were customization of M2M automation and personalized privacy recommendations. This suggests a perception that these factors do not make so much of a difference, or are not as effective in preserving autonomy.

As gathered from the literature, the future vision of the IoT and ambient intelligence place a lot of emphasis on personalization and context-awareness in services. This may sound as if it is beneficial, but the means of providing personalized services may require extensive monitoring and data gathering, as well as processing over time. This is not necessarily agreed upon to be an enabling factor: whether or not it is perceived as beneficial or harmful by someone seems to be more subjective.

According to the results of the surveys, the end-users were more positive than the experts to receiving personalized privacy recommendations and notifications about risks. In the expert survey, E8 (nudges and notifications about risk-averse situations) had the highest percentage of answers in the "somewhat disagree" category. From this it is possible to infer that end-users seem to have more faith in personalization as an enabler, whereas the experts don't or to a smaller extent. This may be because the experts have more knowledge about what is required in terms of data collection and processing to achieve personalization services. It could also be that by sending notifications, it is implied that "the system knows better", which can be perceived by the user as compromising of their autonomy.

5.1.2 Existing Factors that can be Barriers

The factors that were identified as current barriers refer to influences that undermine or hinder the preservation of human autonomy, and factors related to IoT technical developments that could be harmful to humans and society. The most important barriers that were mentioned in all three sources were surveillance and slow regulation; they were identified in the literature and also came up in the expert and end-user study. Other recurring barriers mentioned to some extent in all three sources include proprietary systems that limit user control and hinder open source development, and product design or business models based on collecting and selling user data instead of gathering data for the user exclusively. Generally, the literature, experts, and end-users discussed similar barriers. Some gaps were still brought up by experts, such as ignorance among the public and the lack of technical tools to build genuinely human-centric IoT systems. The development of appropriate tools will require more research, whereas one way to reduce potential ignorance was mentioned throughout the surveys, namely education and awareness.

A noteworthy point regarding proprietary systems and business models based on monetizing user data, is that it is profitable for the companies that produce these devices. It was noted in the expert survey that power and capitalism are the main forces that shape technology design. Tending to the users' needs is not profitable, and this can be why there is a lack of devices that are truly human-centric, and also a lack of research in this area. However, when IoT devices become more than a fun home gadget, when they are incorporated in public spaces, the environment, and being used to carry out societal needs, the focus should not be on profit. Instead of business models that solely pursue financial gains, the focus should shift towards addressing societal needs, environmental concerns, and public welfare, from the beginning of development of the technology and all through implementation and use.

5.2 Autonomy

Turning to the analysis of the prominence of autonomy and its interpretations, the findings illustrate that there is a marked increase (since 2016) in the literature on autonomy, empowerment, and control in the IoT (see Figure 4.1). However, in spite of this observation, many of the technical contributions still stem from techno-deterministic logic with passive mechanisms. For example, the argument used in the articles from the literature review that describe security mechanisms is that improved security enables control, or opposite, control is understood and translated in the literature as protection of privacy and security. There is a difference between passive and active mechanisms: built-in in security and privacy are passive mechanisms, which the users will have to trust are in place to take care of everything. However, there is disagreement among the experts as to whether privacy and security are part of autonomy. The survey results show that around 40% of the experts strongly agree, whereas another 40% somewhat disagree or are neutral to security being an enabler (see Figure 4.2. Additionally, it came up in the open-ended questions that at least one expert sees privacy and security as two different issues. Yet, there is a lot of agreement among the end-users, and a number of the experts state that privacy, security, and control need to be prioritized to enable autonomy.

More importantly, there also exists a gap in the technical translation of autonomy: the need to design for freedom from external influence, as well as the freedom to act. One way to look at autonomy that came up in the expert survey, is to distinguish between negative liberties, i.e., "freedom from", and positive liberties, i.e., "freedom to". It is possible to draw a line between this interpretation and say that the definition of personal autonomy can be categorized as "freedom to" since it emphasizes the possibility performing actions, whereas moral, and, perhaps more relevant, political autonomy, can be said to correspond to "freedom from", since it is specified that one should not be restricted by, but respected by, outside sources. In an everyday-life context, more experts said they interpret autonomy as "freedom to", in contrast to end-users, where more said they interpret the term as "freedom from" (see Figure 4.13). The experts are the ones who have contributed to development and research on the IoT, so their definition would be the one that have been taken into account when translating autonomy technically, which can explain why political autonomy is lacking. Another cause could be that it is difficult to do this, and that there is a lack of tools to build such a protection of "freedom from".

Moreover, in order to build a technical translation of moral autonomy, the users' personal values and moral principles need to be expressed in the technology. According to the literature, one way of doing this would be to build technical capabilities (e.g., AI and machine learning) that can learn ethics and adapt to users' personal values [AF15]. To be more specific, this would require personalization. Perhaps personalization is currently the most feasible option for incorporating moral autonomy, despite its limiting effects on autonomy as mentioned above (see Section 5.1. Future research could investigate whether there is a space for technical developments outside of personalization to protect moral autonomy, such as developing capabilities in the technology for the users to adapt it to reflect their individual values [Dai17].

Futhermore, an interesting finding from the end-user survey is the difference in their definitions of human autonomy in everyday-life context, and in anIoT context. In everyday-life, the majority place emphasis on being free from external restrictions and dictations, i.e., political autonomy, but in the IoT ecosystem, they place importance on being in control of the system and the information shared with it. This coincides with their high agreement rating of transparency as an enabler (see Figure 4.14). It could be so that the end-users are of the opinion that this is a pressing matter, and that the system does not do this as it is now.

Following up on this, a question raised for further discussion is whether it really is necessary to have a common definition of autonomy? There is disagreement in the literature about this. According to Dainow [Dai17], this is a moot topic, and a single definition will not be able to cover all cases. On the other hand, Prunkl [Pru22] advocates the need to agree on this to be able to tackle the uncertainty and complexity surrounding emerging technologies and their implications for the future. Either way, it does not mean that we should scrap the discussion entirely. It is useful to look into diverse perceptions of the term to investigate how it has been implemented currently, what is lacking, and how it should be implemented in the future. Perhaps we do need a single, standardized definition of how autonomy should be translated into the IoT devices, i.e., what needs to be taken into account to be able to say that autonomy is preserved. Put differently, what is important is not necessarily that everyone agrees about a single "correct" definition of the term itself, but that there is a common understanding and agreement on how to protect all the different aspects of human autonomy. As this research strongly implies, political autonomy lacks manifestation in the IoT. In the literature, there is a lack of research on how to protect political autonomy (and to some degree moral autonomy), personal autonomy has gotten most attention.

5.3 The Factors' Impact on Future IoT

In the assessment of the enabler and barrier statements' importance for future IoT, insights from the expert survey revealed that the factors are not likely to be doing anything in isolation, they are interlinked and intertwined. It is difficult to determine the different factors' importance in a quantitative study without making certain simplifications, but it is likely that the factors can have a synergistic effect when combined with each other, but also when combined with other emerging technologies such as AI and machine learning.

Besides, the enablers were found to have a techno-solutionism in their assumptions. The premise that IoT will benefit society will need to account for why, who, and how humans benefit, and whether it is possible to be protected from intelligent surveillance everywhere.

5.3.1 Future Scenario where Human Autonomy is Preserved

Again, the survey results show that the end-users have more confidence than the experts have in the enablers in general, and deem them more important to achieve the optimistic scenario. Moreover, the enablers that have high scores among both end-users and experts, and can thus be said to be most important, are accessibility, transparency and simple conveyance of information, and ethical design principles.

Transparency and information being available are suggested to enable informed decision-making, which was declared in both the expert and end-user survey as important. Truly informed decision-making has some prerequisites: it either requires that the information is easy to understand for all, or that the users have competence about how to understand and use the information, or a combination of these two aspects.

Moreover, insights from the results of the expert survey show that they seem to think most of the enablers are not real enablers. Along with the generally lower scores than the barriers, the notion that some of the enablers will not necessarily give the user what they want, was revealed in the survey. This can be interpreted a situation where what is considered in the literature to be an enabler may not genuinely fulfil its role as an enabler. For instance, one of the experts stated that requiring the user to make an action to preserve their autonomy, actually infringes upon their sense of autonomy. This however, promotes a passive approach to technology. Society is constantly changing, with benefits and drawbacks from new technologies, and sometimes one has to adapt to new developments and changes. Another explanation for enablers not being real, could be the techno-deterministic assumption that technology will always solve the problem, which may not always be the case.

5.3.2 Future Scenario where Human Autonomy is Neglected

The most impactful developments that were rated high in the surveys, as well as mentioned in all three sources (literature review, expert, and user study) are surveillance and systemic biases in how services are provided, although the latter had some internal difference of opinion among the experts (see Table 4.12). Slow regulation and monopoly-tendencies were more emphasized by the end-users, but both groups were concerned with support for ensuring informed consent as a barrier. The results therefore imply that in order to avoid the negative scenario, these are the barriers that need to be addressed. Especially surveillance and systemic biases are the top barriers of concern, as they are becoming more distinct and will need to be dealt with in future technical solutions to protect human autonomy.

The results can also indicate that the experts find the barriers to be more exigent than the end-users. The end-users have faith in the enablers to solve some of the issues, but the experts seem to be more focused on addressing the barriers in order to preserve autonomy. This is supported by the results from the likelihood and desirability ratings of Scenarios 1 and 2, where the experts appear united in the desire of a future where human autonomy is protected, but somewhat pessimistic about the prospects of it.

5.4 General validity of the results

There are at least three aspects that need to be taken into account when considering the general validity of the results from this research. These include the characteristics of the expert panel, the representativeness of the sample in the end-user survey, and the completion times in the end-user survey.

In the expert survey, the panel consisted of mostly academics working in the public sector, except for one researcher in the private sector. It would have been advantageous to include more perspectives, for instance from the industry, policy-making, and government, to represent a more comprehensive portion of expert stakeholders. Additionally, since the topic is about human autonomy, it would be beneficial to have more than the one researcher from social sciences to represent the humanities field.

In the end-user study, a significant proportion of the participants consisted of students, and to some extent individual working in the public or private sector, with a strong interest in technology. The audience was also relatively young, with 73% of participants under the age of 35. While their perspectives are valuable, it is important to acknowledge that this sample does not fully represent the broader population. In order to gain a more comprehensive understanding, it would be beneficial to gather the opinions of non-students, people over 35, and those who do not share that same level of enthusiasm for technology. Further increasing the diversity of perspectives and participants should therefore be a priority for follow-up work on this topic.

Lastly, one limitation of the results from the end-user survey pertains to the amount of time some participants spent completing the end-user survey. While the questionnaire was designed to be completed within a time frame of approximately

10-15 minutes, a subset of respondents completed the survey in significantly shorter periods, ranging from seconds to less than four minutes. This discrepancy in response times suggests the possibility of rushed or incomplete answers, which may have implications for the accuracy and truthfulness of the responses. Furthermore, the presence of response sheets with uniform answers for all questions, such as selecting "Strongly agree" consistently throughout the survey, raises concerns about response reliability. These uniform responses might indicate a lack of careful consideration or an attempt to expedite the survey completion process. It is however worth noting that the majority of respondents fell within the expected completion time range of 10-15 minutes or sometimes even more, suggesting that most participants engaged thoughtfully with the survey. Nevertheless, the variation in response times and patterns necessitates caution when interpreting the survey results.

Chapter 6

Conclusion and Future Research

The main research objectives have been to investigate different perspectives on the definition of human autonomy, and to explore potential enablers and barriers to autonomy in current and future IoT. For this purpose, a systematic literature review, an expert survey and an end-user survey have been conducted. During the mapping of factors from the literature, it became clear that while some factors are distinct barriers or enablers, determining whether a factor is an enabler or a barrier can often be two sides of the same coin. For example, having more transparency in how IoT devices operate would be an enabler of autonomy, whereas having little transparency is a barrier. The results from the surveys suggest that domain experts and end-users prioritize different aspects of autonomy in their definition of the term, at least in the context of everyday-life: End-users place more emphasis on "freedom from" (external influences) than the experts. Moreover, the results imply that the enablers identified in the literature are not necessarily true enablers according to the experts, though the end-users have faith in them. On the barrier side, surveillance was deemed most critical, as it came up repeatedly in all three sources. Systemic biases in the provision of IoT services was also deemed important.

The research in this survey has shed light on potentially new aspects to consider in the development of truly human-centric IoT, by including end-users as stakeholders. It has also highlighted that current solutions fail to provide users with mechanisms needed to exercise their autonomy. Besides, it has underlined the importance of addressing the possibility of mass-surveillance in the IoT.

Research Question 1 has been addressed by examining various interpretations of autonomy in different contexts, to understand what needs prioritizing when attempting to implement this technically. To provide an answer to Research Question 2, a literature review has been performed with the aim of seeking out potential factors that can enable or inhibit autonomy in the IoT. A selection of said factors were then assessed in two surveys to verify the findings from the literature, thereby supporting RQ2, as well as providing answers to the associated Research Question 3. The assessment included experts and end-users indicating their agreement to whether the factors actually are enablers and barriers of autonomy, which is what contributes to RQ2. Furthermore, the participants' judgements on the factors' potential contribution to future scenarios where humans either have autonomy or not are what answers RQ3.

As previously stated, the Internet of Things is growing increasingly pervasive. When technology takes over, there are certain human traits that are at risk of being unlearned if not exercised regularly and properly [BBNT18]. By having an active role and practicing autonomy in the presence of technology, humans can avoid becoming passive kittens, while also enjoying the benefits the Internet of Things has to offer.

6.1 Suggestions to Further Work

It is possible to make greater use of the data collected for this thesis. With such a big dataset from both the literature review and the surveys, time and resource constraints stood in the way of utilizing it to the full. For instance, it could be interesting to make segmentations in the end-user sample based on their degree of scepticism to new technology, to look for patterns or differences within the answers. Another possibility would be to analyze the qualitative survey data in greater detail, for example performing more thematic analysis on recurring factors mentioned in open-ended questions. Moreover, it would be of interest to conduct research on the factors from the literature that were not included in the surveys, and the factors that emerged from the surveys which were not identified in the literature. Besides, since the factors are interlinked, a suggestion could be to find a way to investigate the factors' influence and impact on each other. When it comes to surveying experts, it will be beneficial to incorporate other perspectives than the predominantly academic view this thesis possesses.

The direct next step in researching how human autonomy should be technically translated into the IoT is to explore possible ways to implement a protection of political autonomy, defined as the "freedom from" conception of autonomy. Besides, the pressing issue in which the IoT enables the prospect of mass-surveillance needs to be addressed.

References

[23] «The future of human agency», Pew Research Center: Internet, Science & Tech. (Feb. 24, 2023), [Online]. Available: https://www.pewresearch.org/internet/2023/02/24/the-future-of-human-agency/ (last visited: Aug. 9, 2023).

[ADB+99] G. D. Abowd, A. K. Dey, P. J. Brown, N. Davies, M. Smith, and P. Steggles, «Towards a better understanding of context and context-awareness», in *Handheld and Ubiquitous Computing*, H.-W. Gellersen, Ed., ser. Lecture Notes in Computer Science, Berlin, Heidelberg: Springer, 1999, pp. 304–307.

[AF15] S. A. Applin and M. D. Fischer, «New technologies and mixed-use convergence: How humans and algorithms are adapting to each other», in *2015 IEEE International Symposium on Technology and Society (ISTAS)*, ISSN: 2158-3412, Nov. 2015, pp. 1–6.

[AJD+16] S. B. Allouch, C. Jaschinski, F. Deboeverie, H. Aghajan, and W. Philips, «Lessons learned from SONOPA (SOcial networks for older adults to promote an active life)», *Gerontechnology*, vol. 15, 71s, suppl Nov. 4, 2016. [Online]. Available: https://journal.gerontechnology.org/currentIssueContent.aspx?aid=2362 (last visited: Mar. 16, 2023).

[ALR17] N. Adams, T. D. Little, and R. M. Ryan, «Self-determination theory», in *Development of Self-Determination Through the Life-Course*, M. L. Wehmeyer, K. A. Shogren, T. D. Little, and S. J. Lopez, Eds., Dordrecht: Springer Netherlands, 2017, pp. 47–54. [Online]. Available: https://doi.org/10.1007/978-94-024-1042-6_4 (last visited: Jul. 11, 2023).

[BBNT18] G. Baldini, M. Botterman, R. Neisse, and M. Tallacchini, «Ethical design in the internet of things», *Science and Engineering Ethics*, vol. 24, no. 3, pp. 905–925, Jun. 1, 2018. [Online]. Available: https://doi.org/10.1007/s11948-016-9754-5 (last visited: Mar. 16, 2023).

[BCRW17] R. Bosua, K. Clark, M. Richardson, and J. Webb, «Intelligent warning systems:‘nudges’ as a form of user control for internet of things data collection and use», *Linked Democracy: Artificial Intelligence for Democratic Innovation*, vol. 858, 2017.

[BEG+17] J. Bernal Bernabe, I. Elicegui, E. Gandrille, N. Gligoric, A. Gluhak, C. Hennebert, J. L. Hernandez-Ramos, C. López, A. Manchinu, K. Möessner, M. Nati, C. O'Reilly, N. Palaghias, A. Pintus, L. Sánchez, A. Serra, and R. van Kranenburg, «SocIoTal — the development and architecture of a social IoT framework», in *2017 Global Internet of Things Summit (GIoTS)*, Jun. 2017, pp. 1–6.

[BG20] L. Bertheussen and A. Gastinger, *Litteratursøk, evaluering av informasjon og kildehenvisning - kurs for eksperter i team*, 2020.

[Bha20] P. Bhandari. «Sampling bias and how to avoid it | types & examples», Scribbr. (May 20, 2020), [Online]. Available: https://www.scribbr.com/research-bias/sampling-bias/ (last visited: Jul. 9, 2023).

[BLY13] J. Baskar, H. Lindgren, and C. Yan, «User-control of personalised intelligent environments which support health», in *2013 9th International Conference on Intelligent Environments*, Jul. 2013, pp. 270–273.

[BMG15] P. Bisson, F. Martinelli, and R. Granadino, «Cybersecurity strategic research agenda-sra», *European Network and Information Security (NIS) Platform-NISP-Working Group*, vol. 3, pp. 1–201, 2015.

[Bon] E. Bonabeau. «Agent-based modeling: Methods and techniques for simulating human systems». (), [Online]. Available: https://www.pnas.org/doi/10.1073/pnas.082080899 (last visited: Jul. 2, 2023).

[BP06] J.-C. Burgelman and Y. Punie, «Information, society and technology», in *True Visions: The Emergence of Ambient Intelligence*, E. Aarts and J. Encarnação, Eds., Berlin, Heidelberg: Springer, 2006, pp. 17–33. [Online]. Available: https://doi.org/10.1007/978-3-540-28974-6_2 (last visited: Mar. 16, 2023).

[BW18] S. Buss and A. Westlund, «Personal Autonomy», in *The Stanford Encyclopedia of Philosophy*, E. N. Zalta, Ed., Spring 2018, Metaphysics Research Lab, Stanford University, 2018. (last visited: Aug. 8, 2023).

[CCFS16] B. Carminati, P. Colombo, E. Ferrari, and G. Sagirlar, «Enhancing user control on personal data usage in internet of things ecosystems», in *2016 IEEE International Conference on Services Computing (SCC)*, Jun. 2016, pp. 291–298.

[CDMR19] L. Coppolino, S. D'Antonio, G. Mazzeo, and L. Romano, «A comprehensive survey of hardware-assisted security: From the edge to the cloud», *Internet of Things*, vol. 6, p. 100 055, Jun. 1, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660519300101 (last visited: Mar. 16, 2023).

[CFS+14] C. Y. Chen, J. H. Fu, T. Sung, P.-F. Wang, E. Jou, and M.-W. Feng, «Complex event processing for the internet of things and its applications», in *2014 IEEE International Conference on Automation Science and Engineering (CASE)*, ISSN: 2161-8089, Aug. 2014, pp. 1144–1149.

[CGM+21] C. S. Constantinou, T. Gurung, H. Motamedian, C. Mavromoustakis, and G. Mastorakis, «New ambient assisted living technology: A narrative review», in *Intelligent Technologies for Internet of Vehicles*, ser. Internet of Things, N. Magaia, G. Mastorakis, C. Mavromoustakis, E. Pallis, and E. K. Markakis, Eds., Cham: Springer International Publishing, 2021, pp. 487–499. [Online]. Available: https://doi.org/10.1007/978-3-030-76493-7_16 (last visited: Mar. 16, 2023).

[CLC+18] A. Crabtree, T. Lodge, J. Colley, C. Greenhalgh, K. Glover, H. Haddadi, Y. Amar, R. Mortier, Q. Li, J. Moore, L. Wang, P. Yadav, J. Zhao, A. Brown, L. Urquhart, and D. McAuley, «Building accountability into the internet of things: The IoT databox model», *Journal of Reliable Intelligent Environments*, vol. 4, no. 1, pp. 39–55, Apr. 1, 2018. [Online]. Available: https://doi.org/10.1007/s40860-018-0054-5 (last visited: May 24, 2023).

[Dai17] B. Dainow, «Threats to autonomy from emerging ICTs», *Australasian Journal of Information Systems*, vol. 21, Nov. 26, 2017, Publisher: Australian Computer Society. [Online]. Available: https://journal.acs.org.au/index.php/ajis/article/view/1438 (last visited: Mar. 16, 2023).

[DAM17] G. Desolda, C. Ardito, and M. Matera, «Empowering end users to customize their smart environments: Model, composition paradigms, and domain-specific tools», *ACM Transactions on Computer-Human Interaction*, vol. 24, no. 2, 12:1–12:52, Apr. 27, 2017. [Online]. Available: https://dl.acm.org/doi/10.1145/3057859 (last visited: Mar. 16, 2023).

[DeC18] M. DeCarlo, «11.2 strengths and weaknesses of survey research», Aug. 7, 2018, Book Title: Scientific Inquiry in Social Work Publisher: Open Social Work Education. [Online]. Available: https://pressbooks.pub/scientificinquiryinsocialwork/chapter/11-2-strengths-and-weaknesses-of-survey-research/ (last visited: Jul. 10, 2023).

[DHD19] H. Damghani, H. Hosseinian, and L. Damghani, «Cryptography review in IoT», *Information and Communication Technology*, 2019.

[Dic02] O. Dictionaries, *Factor*, in *The Oxford Essential Dictionary of the U.S. Military*, Oxford University Press, 2002. [Online]. Available: https://www.oxfordreference.com/display/10.1093/acref/9780199891580.001.0001/acref-9780199891580-e-2802;jsessionid=C851D84E4B4EB65A024E2AB421A93A6C (last visited: Aug. 8, 2023).

[Dim16] T. Dimitriou, «Key evolving RFID systems: Forward/backward privacy and ownership transfer of RFID tags», *Ad Hoc Networks*, vol. 37, pp. 195–208, Feb. 1, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870515001857 (last visited: Mar. 16, 2023).

[Dr 20] M. P. G. Dr. Chetlal Prasad, «Educational impact on the society», *International Journal of Novel Research in Education and Learning*, vol. 7, pp. 1–7, Nov. 2020.

[Dwo88] G. Dworkin, *The Theory and Practice of Autonomy* (Cambridge Studies in Philosophy). Cambridge University Press, 1988.

[Eco17] A. A. Economides, «User perceptions of internet of things (IoT) systems», in *E-Business and Telecommunications*, M. S. Obaidat, Ed., ser. Communications in Computer and Information Science, Cham: Springer International Publishing, 2017, pp. 3–20.

[EFCS19] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, «A survey of internet of things (IoT) authentication schemes», *Sensors*, vol. 19, no. 5, p. 1141, Jan. 2019, Number: 5 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/1424-8220/19/5/1141 (last visited: Jul. 1, 2023).

[Els] Elsevier. «Why systematic reviews matter», Elsevier Connect. (), [Online]. Available: https://www.elsevier.com/connect/authors-update/why-systematic-reviews-matter (last visited: Jun. 22, 2023).

[FAMC22] J. François, A.-F. Audrain-Pontevia, L. Menvielle, and N. Chevalier, «Empowering health care consumers in the era of internet of things», *International Journal of Consumer Studies*, vol. n/a, n/a Oct. 30, 2022, _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/ijcs.12887. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/ijcs.12887 (last visited: Mar. 16, 2023).

[FDD+19] D. Fink-Hafner, T. Dagen, M. Doušak, M. Novak, and M. Hafner-Fink, «Delphi method: Strengths and weaknesses», *Advances in Methodology and Statistics*, vol. 2, pp. 1–19, Nov. 1, 2019.

[FS15] C. Fernandes and V. Sivaraman, «It's only the beginning: Metadata retention laws and the internet of things», *Australian Journal of Telecommunications and the Digital Economy*, vol. 3, p. 47, Sep. 28, 2015.

[G] N. G. «How many iot devices are there in 2023? [all you need to know]», Techjury. (), [Online]. Available: https://techjury.net/blog/how-many-iot-devices-are-there/#gref (last visited: Aug. 11, 2023).

[GB14] D. Gallego and S. Bueno, «Exploring the application of the delphi method as a forecasting tool in information systems and technologies research», *Technology Analysis & Strategic Management*, vol. 26, no. 9, pp. 987–999, Oct. 21, 2014, Publisher: Routledge _eprint: https://doi.org/10.1080/09537325.2014.941348. [Online]. Available: https://doi.org/10.1080/09537325.2014.941348 (last visited: Jun. 13, 2023).

[GVK19] R. Garg, S. Varadi, and A. Kertesz, «Legal considerations of IoT applications in fog and cloud environments», in *2019 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)*, ISSN: 2377-5750, Feb. 2019, pp. 193–198.

[HMM10] G. P. Hancke, K. Markantonakis, and K. E. Mayes, «Security challenges for user-oriented rfid applications within the" internet of things"», *Journal of Internet Technology*, vol. 11, no. 3, pp. 307–313, 2010.

[HS20] N. A. Hussein and M. I. Shujaa, «DNA computing based stream cipher for internet of things using MQTT protocol», *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 1, pp. 1035–1042, Feb. 1, 2020, Number: 1. [Online]. Available: https://ijece.iaescore.com/index.php/IJECE/article/view/21070 (last visited: Mar. 16, 2023).

[HWJ20] L.-V. Herm, J. Wanner, and C. Janiesch, «Bridging the architectural gap in smart homes between user control and digital automation», in *Designing for Digital Transformation. Co-Creating Services with Citizens and Industry*, S. Hofmann, O. Müller, and M. Rossi, Eds., ser. Lecture Notes in Computer Science, Cham: Springer International Publishing, 2020, pp. 376–381.

[JCP17] W. Jang, A. Chhabra, and A. Prasad, «Enabling multi-user controls in smart home devices», in *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, ser. IoTS&amp;P '17, New York, NY, USA: Association for Computing Machinery, Nov. 3, 2017, pp. 49–54. [Online]. Available: https://dl.acm.org/doi/10.1145/3139937.3139941 (last visited: Mar. 16, 2023).

[JKH20] H. Jin, S. Kumar, and J. Hong, «Providing architectural support for building privacy-sensitive smart home applications», in *Adjunct Proceedings of the 2020 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2020 ACM International Symposium on Wearable Computers*, ser. UbiComp-ISWC '20, New York, NY, USA: Association for Computing Machinery, Sep. 12, 2020, pp. 212–217. [Online]. Available: https://dl.acm.org/doi/10.1145/3410530.3414328 (last visited: Mar. 16, 2023).

[Kar21] A. Karale, «The challenges of IoT addressing security, ethics, privacy, and laws», *Internet of Things*, vol. 15, p. 100 420, Sep. 1, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660521000640 (last visited: Jul. 8, 2023).

[Kur21] K. Kuru, «Conceptualisation of human-on-the-loop haptic teleoperation with fully autonomous self-driving vehicles in the urban environment», *IEEE Open Journal of Intelligent Transportation Systems*, vol. 2, pp. 448–469, 2021, Conference Name: IEEE Open Journal of Intelligent Transportation Systems.

[KZDB19] P. Kelly, M. Zallio, B. Duarte, and D. Berry, «Design for enabling technologies. a framework to empower multi-level user engagement», in *Advances in Design for Inclusion*, G. Di Bucchianico, Ed., ser. Advances in Intelligent Systems and Computing, Cham: Springer International Publishing, 2019, pp. 65–74.

[LBC18] A. J. Lee, J. T. Biehl, and C. Curry, «Sensing or watching? balancing utility and privacy in sensing systems via collection and enforcement mechanisms», in *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies*, ser. SACMAT '18, New York, NY, USA: Association for Computing Machinery, Jun. 7, 2018, pp. 105–116. [Online]. Available: https://dl.acm.org/doi/10.1145/3205977.3205983 (last visited: Mar. 16, 2023).

[LE06] Y. Levy and T. J. Ellis, «A systems approach to conduct an effective literature review in support of information systems research», *Informing Science Journal*, vol. 9, no. 1, pp. 181–212, 2006.

[Lei23] S. Lein, «Exploring the enablers and barriers of human autonomy in iot», Department of Information Security, Communication Technology, NTNU – Norwegian University of Science, and Technology, Project report in TTM4502, Jan. 2023.

[LS21] A. Laitinen and O. Sahlgren, «AI systems and respect for human autonomy», *Frontiers in Artificial Intelligence*, vol. 4, 2021. [Online]. Available: https://www.frontiersin.org/articles/10.3389/frai.2021.705164 (last visited: Jun. 4, 2023).

[LSE22] S. Lythreatis, S. K. Singh, and A.-N. El-Kassar, «The digital divide: A review and future research agenda», *Technological Forecasting and Social Change*, vol. 175, p. 121 359, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0040162521007903.

[Lup13] D. Lupton, «The digitally engaged patient: Self-monitoring and self-care in the digital health era», *Social Theory & Health*, vol. 11, no. 3, pp. 256–270, Aug. 1, 2013. [Online]. Available: https://doi.org/10.1057/sth.2013.10 (last visited: Jun. 30, 2023).

[Mas21] MassChallenge. «Haptic technology: The future of engagement?», MassChallenge. (Sep. 23, 2021), [Online]. Available: https://masschallenge.org/articles/haptic-technology/ (last visited: Jun. 28, 2023).

[MKAB19] Z. Maamar, E. Kajan, M. Asim, and T. Baker Shamsa, «Open challenges in vetting the internet-of-things», *Internet Technology Letters*, vol. 2, no. 5, e129, 2019, _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/itl2.129. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/itl2.129 (last visited: Mar. 16, 2023).

[MSS16] I. Miles, O. Saritas, and A. Sokolov, *Foresight for Science, Technology and Innovation* (Science, Technology and Innovation Studies). Springer International Publishing Switzerland, 2016.

[MTB22] S. McDonald, D. Towey, and V. Brusic, «Social impact of smart environments: Software engineering perspectives and challenges», in *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*, ISSN: 0730-3157, Jun. 2022, pp. 1592–1597.

[NBS+15] R. Neisse, G. Baldini, G. Steri, Y. Miyake, S. Kiyomoto, and A. R. Biswas, «An agent-based framework for informed consent in the internet of things», Dec. 14, 2015.

[Nik22a] K. Nikolopoulou. «What is convenience sampling? | definition & examples», Scribbr. (Aug. 9, 2022), [Online]. Available: https://www.scribbr.com/methodology/convenience-sampling/ (last visited: Jul. 9, 2023).

[Nik22b] K. Nikolopoulou. «What is selection bias? | definition & examples», Scribbr. (Sep. 30, 2022), [Online]. Available: https://www.scribbr.com/research-bias/selection-bias/ (last visited: Jul. 9, 2023).

[NO16] J. Nolin and N. Olson, «The internet of things and convenience», *Internet Research*, vol. 26, no. 2, P. S. C. Professor Pan Wang Professor Ling Li, Ed., pp. 360–376, Jan. 1, 2016, Publisher: Emerald Group Publishing Limited. [Online]. Available: https://doi.org/10.1108/IntR-03-2014-0082 (last visited: Mar. 16, 2023).

[NZS15] D. S. Nunes, P. Zhang, and J. Sa Silva, «A survey on human-in-the-loop applications towards an internet of all», *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 944–965, 2015. [Online]. Available: https://ieeexplore.ieee.org/document/7029083/ (last visited: Jun. 30, 2023).

[oPub16] C. U. M. S. of Public Health. «Agent-based modeling», Columbia University Mailman School of Public Health. (Aug. 3, 2016), [Online]. Available: https://www.publichealth.columbia.edu/research/population-health-methods/agent-based-modeling (last visited: Jul. 2, 2023).

[OS22] S. Oppl and C. Stary, «Motivating users to manage privacy concerns in cyber-physical settings—a design science approach considering self-determination theory», *Sustainability*, vol. 14, no. 2, p. 900, Jan. 2022, Number: 2 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/2071-1050/14/2/900 (last visited: Mar. 16, 2023).

[PC99] N. Page and C. E. Czuba. «Empowerment: What is it?» (Oct. 1999), [Online]. Available: https://archives.joe.org/joe/1999october/comm1.php (last visited: Aug. 8, 2023).

[PFH15] J. P. Pienaar, R. M. Fisher, and G. P. Hancke, «Smartphone: The key to your connected smart home», in *2015 IEEE 13th International Conference on Industrial Informatics (INDIN)*, ISSN: 2378-363X, Jul. 2015, pp. 999–1004.

[Pru22] C. Prunkl, «Human autonomy in the age of artificial intelligence», *Nature Machine Intelligence*, vol. 4, no. 2, pp. 99–101, Feb. 23, 2022. [Online]. Available: https://www.nature.com/articles/s42256-022-00449-9 (last visited: Mar. 16, 2023).

[Pun05] Y. Punie, «The future of ambient intelligence in europe:the need for more everyday life», *Communication and Stratégies*, vol. 57, Jan. 1, 2005.

[PZ21] K. Y. Ponomarev and A. A. Zaharov, «Framework for processing medical data and secure machine learning in internet of medical things», in *Futuristic Trends in Network and Communication Technologies*, P. K. Singh, G. Veselov, A. Pljonkin, Y. Kumar, M. Paprzycki, and Y. Zachinyaev, Eds., ser. Communications in Computer and Information Science, Singapore: Springer, 2021, pp. 264–275.

[Ric13] N. M. Richards. «The dangers of surveillance», Harvard Law Review. (May 20, 2013), [Online]. Available: https://harvardlawreview.org/print/vol-126/the-dangers-of-surveillance/ (last visited: Jul. 29, 2023).

[RJJ+22] R. Raghu, V. Jayaraman, J. Jayaraman, S. S. V. Nukala, and V. G. Díaz, «A multi-layered edge-secured cloud framework for healthcare monitoring in old-age homes using smart systems driven by comprehensive user interaction», *International Journal of Safety and Security Engineering*, vol. 12, no. 4, pp. 449–457, Aug. 31, 2022. [Online]. Available: https://www.iieta.org/journals/ijsse/paper/10.18280/ijsse.120405 (last visited: Mar. 16, 2023).

[RM06] Y. Rogers and H. Muller, «A framework for designing sensor-based interactions to promote exploration and reflection in play», *International Journal of Human-Computer Studies*, vol. 64, no. 1, pp. 1–14, Jan. 1, 2006. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1071581905001126 (last visited: Mar. 16, 2023).

[RMI22] M. Rana, Q. Mamun, and R. Islam, «Lightweight cryptography in IoT networks: A survey», *Future Generation Computer Systems*, vol. 129, pp. 77–89, Apr. 1, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X21004404 (last visited: Jul. 1, 2023).

[Roa23] C. Roach. «What is digital rights management (DRM)? (the definitive guide)». (May 5, 2023), [Online]. Available: https://www.digitalguardian.com/blog/what-digital-rights-management (last visited: Jul. 25, 2023).

[RR12] S. Roopa and M. Rani, «Questionnaire designing for a survey», *Journal of Indian Orthodontic Society*, vol. 46, no. 4, pp. 273–277, Oct. 1, 2012, Publisher: SAGE Publications India. [Online]. Available: https://journals.sagepub.com/doi/abs/10.5005/jp-journals-10021-1104 (last visited: Jun. 22, 2023).

[RW01] G. Rowe and G. Wright, «Expert opinions in forecasting: The role of the delphi technique», *International Series in Operations Research and Management Science*, Jan. 1, 2001.

[RZL13] R. Roman, J. Zhou, and J. Lopez, «On the features and challenges of security and privacy in distributed internet of things», *Computer Networks*, Towards a Science of Cyber Security, vol. 57, no. 10, pp. 2266–2279, Jul. 5, 2013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128613000054 (last visited: Jun. 30, 2023).

[Röc10] C. Röcker, «Socially dependent interaction in smart spaces», in *2010 International Conference on Mechanical and Electrical Technology*, Sep. 2010, pp. 314–318.

[SCD22] M. Sitesh, K. Cormican, and C. Dhanapathi, «Analysis of critical success factors to mitigate privacy risks in IoT devices», *Procedia Computer Science*, International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies 2021, vol. 196, pp. 191–198, Jan. 1, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050921022286 (last visited: Mar. 16, 2023).

[SCN19] J. Singh, J. Cobbe, and C. Norval, «Decision provenance: Harnessing data flow for accountable systems», *IEEE Access*, vol. 7, pp. 6562–6574, 2019, Conference Name: IEEE Access.

[SGP+20] C. Savaglio, M. Ganzha, M. Paprzycki, C. Bădică, M. Ivanović, and G. Fortino, «Agent-based internet of things: State-of-the-art and research challenges», *Future Generation Computer Systems*, vol. 102, pp. 1038–1053, Jan. 1, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X19312282 (last visited: Jul. 2, 2023).

[SHK+21] L. Sineviciene, L. Hens, O. Kubatko, I. Dehtyarova, L. Melnyk, and S. Fedyna, «Socio-economic and cultural effects of disruptive industrial technologies for sustainable development», *International Journal of Global Energy Issues*, vol. 43, p. 284, Jan. 1, 2021.

[SKL18] S. Spiekermann-Hoff, J. Korunovska, and M. Langheinrich, «Understanding engineers' drivers and impediments for ethical system development: The case of privacy and security engineering», English, WU Vienna University of Economics and Business, WorkingPaper, 2018.

[SNCL15] R. Skinner, R. R. Nelson, W. W. Chin, and L. Land, «The delphi method research strategy in studies of information systems», *Communications of the Association for Information Systems*, vol. 37, 2015. [Online]. Available: https://aisel.aisnet.org/cais/vol37/iss1/2 (last visited: Jun. 13, 2023).

[Sny19] H. Snyder, «Literature review as a research methodology: An overview and guidelines», *Journal of Business Research*, vol. 104, pp. 333–339, Nov. 1, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0148296319304564 (last visited: Jun. 21, 2023).

[Spi18] S. Spiekermann, «Carousel kittens: The case for a value-based IoT», *IEEE Pervasive Computing*, vol. 17, no. 2, pp. 62–65, Apr. 2018, Conference Name: IEEE Pervasive Computing.

[SPKZ21] Y. Shanmugarasa, H.-Y. Paik, S. S. Kanhere, and L. Zhu, «Towards automated data sharing in personal data stores», in *2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, Mar. 2021, pp. 328–331.

[SS22] Y. Singh and A. Singh, «Lightweight cryptography approach for multifactor authentication in internet of things», in *2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon)*, Oct. 2022, pp. 1–7.

[STHK20] O. R. Sanchez, I. Torre, Y. He, and B. P. Knijnenburg, «A recommendation approach for user privacy preferences in the fitness domain», *User Modeling and User-Adapted Interaction*, vol. 30, no. 3, pp. 513–565, Jul. 1, 2020. [Online]. Available: https://doi.org/10.1007/s11257-019-09246-3 (last visited: Mar. 16, 2023).

[Tec] TechTarget. «What is context awareness? | definition from TechTarget», WhatIs.com. (), [Online]. Available: https://www.techtarget.com/whatis/definition/context-awareness (last visited: Jul. 1, 2023).

[Uğu23] Ö. Uğuz. «The internet of things: Legal considerations and regulatory framework», LAWELS. (May 21, 2023), [Online]. Available: https://lawels.com/en/2023/05/21/the-internet-of-things-legal-considerations-and-regulatory-framework/ (last visited: Jul. 8, 2023).

[VO14] M. Van Kleek and K. OHara, «The future of social is personal: The potential of the personal data store», in *Social Collective Intelligence: Combining the Powers of Humans and Machines to Build a Smarter Society*, ser. Computational Social Sciences, D. Miorandi, V. Maltese, M. Rovatsos, A. Nijholt, and J. Stewart, Eds., Cham: Springer International Publishing, 2014, pp. 125–158. [Online]. Available: https://doi.org/10.1007/978-3-319-08681-1_7 (last visited: Aug. 2, 2023).

[YAP+23] K. F. Ystgaard, L. Atzori, D. Palma, P. E. Heegaard, L. E. Bertheussen, M. R. Jensen, and K. De Moor, «Review of the theory, principles, and design requirements of human-centric internet of things (IoT)», *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 3, pp. 2827–2859, Mar. 1, 2023. [Online]. Available: https://doi.org/10.1007/s12652-023-04539-3 (last visited: Jun. 15, 2023).

[YD23] K. F. Ystgaard and K. De Moor, «Future scoping of truly human-centric IoT and intelligent networks: A foresight approach», in *Proceedings of the 12th International Conference on the Internet of Things*, ser. IoT '22, New York, NY, USA: Association for Computing Machinery, Jan. 5, 2023, pp. 81–87. [Online]. Available: https://dl.acm.org/doi/10.1145/3567445.3567452 (last visited: Mar. 22, 2023).

[YH21] H. Younis and J. H. Hansen, «Challenges in real-time-embedded IoT command recognition», in *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*, Jun. 2021, pp. 848–851.

[ZAD20] T. Zachariah, J. Adkins, and P. Dutta, «Browsing the web of connectable things.», in *EWSN*, 2020, pp. 49–60.

[AAA21] M. A. F. Al-Husainy, B. Al-Shargabi, and S. Aljawarneh, «Lightweight cryptography system for IoT devices using DNA», *Computers and Electrical Engineering*, vol. 95, p. 107 418, Oct. 1, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0045790621003827 (last visited: Jul. 1, 2023).

Appendix A
Search Syntax

The next page contains the full search syntax in Table A.1, this includes the name of the databases, and the date of each database search in the systematic literature review. DB stands for database, and WoS stands for Web of Science. The "n" column displays the number of hits each search yielded.

Table A.1: Full search syntax.

DB	Date	n	Syntax
Scopus	03/06/23	55	((TITLE-ABS-KEY ("human autonomy" OR "user autonomy" OR "human agency" OR "user agency" OR "human empowerment" OR "user empowerment" OR "user control" OR "human control"))) AND (TITLE-ABS-KEY("driver*" OR "enabler*" OR "facilitator*" OR "barrier*" OR "inhibitor" OR "risk" OR "threat" OR "impediment" OR "factor" OR "aspect" OR "characteristic")) AND (TITLE-ABS-KEY("internet of things" OR "IoT" OR "intelligent environment" OR "sensor technology"))
IEEE	03/06/23	5	((("All Metadata": "human autonomy" OR "user autonomy" OR "human agency" OR "user agency" OR "human empowerment" OR "user empowerment" OR "user control" OR "human control") AND ("All Metadata": "IoT" OR "Internet of Things" OR "intelligent environment" OR "sensor technology") AND ("All Metadata": "driver" OR "enabler" OR "facilitator" OR "barrier" OR "inhibitor" OR "risk" OR "threat" OR "impediment" OR "factor" OR "aspect" OR "characteristic")))
ACM	03/15/23	6	(("human autonomy" OR "user autonomy" OR "human agency" OR "user agency" OR "human empowerment" OR "user empowerment" OR "user control" OR "human control") AND ("IoT" OR "Internet of Things" OR "intelligent environment" OR "sensor technology") AND (driver OR enabler OR facilitator OR barrier OR inhibitor OR risk OR threat OR impediment OR factor OR aspect OR characteristic))
WoS	03/01/23	18	((TS=((“human autonomy” OR “user autonomy” OR “human agency” OR “user agency” OR “human empowerment” OR “user empowerment” OR “user control” OR “human control”) AND (IoT OR “Internet of Things” OR "intelligent environment" OR "sensor technology") AND (driver OR enabler OR facilitator OR barrier OR inhibitor OR risk OR threat OR impediment OR factor OR aspect OR characteristic))))

Appendix B
Selection Criteria

The next two pages contain the selection protocol with the criteria used for the inclusion and exclusion of articles in the systematic literature review.

Selection protocol

Title:

Exploring the Enablers and Barriers of Human Autonomy in IoT

Abstract:

The project aims to explore the current main factors that enable and inhibit human autonomy in the Internet of Things (IoT), and to examine what their significance will be for ensuring human autonomy in future network technology which strives to be truly human-centric.

The purpose of this literature review is to systematically review literature on human autonomy in the context of the Internet of Things, in order to:

- Map the main current technical and non-technical factors (and underlying mechanisms) that enable human autonomy in IoT.
- Map the main current technical and non-technical factors (and underlying mechanisms) that inhibit human autonomy in IoT.
- Map factors that influence human autonomy in IoT??

Inclusion criteria:

1. Include literature that discusses aspects related to human autonomy in IoT. Relevant aspects include, but are not limited to:

- Technical and non-technical mechanisms that preserve and/or enhance user autonomy.
- Technical and non-technical mechanisms that intend to empower the user, give control to the user, give agency to the user.
- Technical and non-technical mechanisms that decrease and/or hinder user autonomy.

2. Include literature that discusses, or aims to gain a common definition of, human autonomy in the context of IoT.

- Literature discussing the technical/non-technical requirements for human autonomy, and how we can know or verify whether these are fulfilled.

3. Include literature that discusses a factor or several factors that influence the degree of human autonomy in IoT.

- Factor(s) is/are explicitly identified and discussed, and reasoning is provided.
- Factor(s) is/are implicitly identified, and one can infer why it enables/inhibits human autonomy.

- Factors are aspects that influence control, empowerment, agency and/or autonomy.

4. Include literature that utilizes an ethical design approach.

Exclusion criteria:

1. Exclude literature that only refer to human autonomy aspects superficially.

- Autonomy aspect is only mentioned once or used as a buzzword.

2. Exclude literature that primarily concerns business implications or technical performance.

- Exclude studies that primarily discuss human autonomy from a business user perspective.

3. Exclude literature that does not discuss aspects related to human autonomy in the IoT. Relevant aspects are the same as in inclusion criterion 1.

Appendix C
List of Articles

The following pages contain Table C.1, the list of articles that were deemed relevant and therefore included in the systematic literature review. The "Ref" column contains a link to the article in the list of references, where additional information such as name of the authors and year of publication can be found.

Table C.1: List of articles in the literature review.

Title	Ref
Threats to Autonomy from Emerging ICTs	[Dai17]
Intelligent Warning Systems: 'Nudges' as a Form of User Control for Internet of Things Data Collection and Use	[BCRW17]
New technologies and mixed-use convergence: How humans and algorithms are adapting to each other	[AF15]
A framework for designing sensor-based interactions to promote exploration and reflection in play	[RM06]
A comprehensive survey of hardware-assisted security: From the edge to the cloud	[CDMR19]
A Multi-Layered Edge-Secured Cloud Framework for Healthcare Monitoring in Old-Age Homes Using Smart Systems Driven by Comprehensive User Interaction	[RJJ+22]
A recommendation approach for user privacy preferences in the fitness domain	[STHK20]
Analysis of critical success factors to mitigate privacy risks in IoT Devices	[SCD22]
Bridging the Architectural Gap in Smart Homes Between User Control and Digital AutomationThreats to Autonomy from Emerging ICTs	[HWJ20]

Browsing the Web of Connectable Things	[ZAD20]
Challenges in real-time-embedded IoT Command Recognition	[YH21]
Conceptualisation of Human-on-the-Loop Haptic Teleoperation With Fully Autonomous Self-Driving Vehicles in the Urban Environment	[Kur21]
Decision Provenance: Harnessing Data Flow for Accountable System	[SCN19]
Design for Enabling Technologies. A Framework to Empower Multi-level User Engagement	[KZDB19]
DNA computing based stream cipher for internet of things using MQTT protocol	[HS20]
Empowering End Users to Customize their Smart Environments: Model, Composition Paradigms, and Domain-Specific Tools	[DAM17]
Empowering health care consumers in the era of Internet of Things	[FAMC22]
Enabling Multi-user Controls in Smart Home Devices	[JCP17]
Enhancing user control on personal data usage in Internet of Things ecosystems	[CCFS16]
Ethical Design in the Internet of Things	[BBNT18]
Framework for Processing Medical Data and Secure Machine Learning in Internet of Medical Things	[PZ21]
Information, Society and Technology	[BP06]
It's only the beginning: Metadata Retention laws and the Internet of Things	[FS15]
Key evolving RFID systems: Forward/backward privacy and ownership transfer of RFID tags	[Dim16]
Legal Considerations of IoT Applications in Fog and Cloud Environments	[GVK19]
Lessons learned from SONO PA (SOcial Networks for Older adults to Promote an Active life)	[AJD+16]
Lightweight Cryptography Approach for Multifactor Authentication in Internet of Things	[SS22]
Motivating Users to Manage Privacy Concerns in Cyber-Physical Settings—A Design Science Approach Considering Self-Determination Theory	[OS22]
New Ambient Assisted Living Technology: A Narrative Review	[CGM+21]
Open challenges in vetting the internet-of-things	[MKAB19]

Providing architectural support for building privacy-sensitive smart home applications	[JKH20]
Sensing or Watching? Balancing Utility and Privacy in Sensing Systems via Collection and Enforcement Mechanisms	[LBC18]
Smartphone: The Key to your Connected Smart Home	[PFH15]
Socially Dependent Interaction in Smart Spaces	[Röc10]
Socio-economic and cultural effects of disruptive industrial technologies for sustainable development	[SHK+21]
SocIoTal-The Development and Architecture of a Social IoT framework	[BEG+17]
The Future of Ambient Intelligence in Europe:The Need for More Everyday Life	[Pun05]
The Internet of Things and convenience	[NO16]
Towards Automated Data Sharing in Personal Data Stores	[SPKZ21]
User Perceptions of Internet of Things (IoT) Systems	[Eco17]
User-Control of Personalised Intelligent Environments which Support Health	[BLY13]

Appendix D
Survey Invitation

The following page contains the survey invitation text that was published in various channels with the aim of recruiting participants to the end-user survey.

Are you fascinated by the potential of smart environment technology?

Informasjonssikkerhet (MTKOM-IS) 07.06.2023 Av Silje Kløften Lein

Or afraid of its consequences for the future?

A smart environment is one enriched with technology in the form of sensors, actuators, processors, and information terminals. Share your insights on the aspects influencing human control, self-direction, and empowerment in the world of smart environments.

Your opinions are invaluable for my master's thesis research, as I seek to understand the complexities of human interaction with smart environments.

By taking just 10 minutes to complete this anonymous survey, you can contribute to the advancement of knowledge in this field and influence the design of future smart environment technologies.

If you are interested in participating, kindly fill out this questionnaire:

https://nettskjema.no/a/346849

Be part of shaping the future of technology!

Best,
Silje Kløften Lein
Master's student, IIK

PS: I am also looking for experts with a bit more knowledge on the topic of smart environments to participate in an expert survey. If you know of someone or consider yourself to be one, please email me on siljkle@stud.ntnu.no for more information.

Oppdatert: 13.15 07.06.2023 Åpne saken i ny fane/vindu

Appendix E
Expert Survey

The subsequent pages contain the questionnaire that was used in the expert survey. In the multiple choice questions, the checkboxes represent mutually exclusive answer options.

Expert survey - The Future of Human Autonomy: Predicting Trends and Shaping IoT Development

Mandatory fields are marked with a star *

This survey is a part of a study exploring factors that influence human autonomy in the Internet of Things (IoT).

The survey is separated into four parts:

1. Demographics and familiarity with IoT
2. Your interpretation of the term 'human autonomy'
3. Potential enablers of human autonomy
4. Potential barriers to human autonomy

It takes around **10-15 minutes** to fill out the survey. All information will be treated confidentially. The technical implementation of the survey is done in Nettskjema and the data are gathered completely anonymously.

If you have any questions or comments related to the survey, contact Silje Kløften Lein (siljkle@stud.ntnu.no), master's student in communication technology at the Norwegian University of Science and Technology (NTNU).

Section: Demographics

Please specify your gender. *

- □ Female
- □ Male
- □ Non-binary
- □ Other
- □ Prefer not to say

Which age group do you belong to? *

Please select the option that best represents your age range.

- □ 18-24
- □ 25-34
- □ 35-44
- □ 45-54
- □ 55-64
- □ 65 or above

Where are you located? *

Please indicate your permanent residence.

- □ Norway
- □ Europe (outside of Norway)
- □ North America
- □ Africa
- □ South America

- □ Asia
- □ Australia
- □ Other

What is the highest level of education you have completed? *

Please select the option that best describes your educational background.

- □ Upper Secondary School/High School Diploma
- □ Bachelor’s Degree
- □ Master’s Degree
- □ Doctorate/Ph.D
- □ Other

Please state your job title (i.e., IoT researcher, Senior Data Scientist, Associate professor in sociology, etc.) *

Do not include the name of your workplace or any personal information.

Which sector do you work in? *

- □ Public
- □ Private

How many years of experience do you have working within your field? *

- □ Less than 1 year
- □ 1-5 years
- □ 5-10 years
- □ 10-15 years
- □ 15-20 years
- □ More than 20 years

Have you developed or contributed to the development or research of intelligent environment technologies (i.e. Smart home systems, energy management systems, health-care systems that are autonoumous and intelligent) *

- □ Yes
- □ No
- □ Maybe

Section: Your interpretation of “human autonomy”

The following section contains some open questions. Please fill out these before proceeding to the next section.
The term 'human autonomy' is described with different definitions in literature. This research aims to map the correspondence between definitions from literature and expert's perception of the term.

How do you interpret the concept 'human autonomy' in the context of everyday life?*

Please describe your view in a few sentences. There is no right or wrong answer to this question, we are interested in your perception of the term.

In your opinion, how does human autonomy manifest in a technical context within the IoT ecosystem? *

Please describe your view in a few sentences. There is no right or wrong answer to this question, we are interested in your perception of the term.

In the following two sections, a selection of statements will be introduced. The statements concern factors that influence human autonomy in IoT. The factors are retrieved from a literature review conducted in March 2023, with literary works obtained from the IEEE, Scopus, ACM and Web of Science databases.

Section: Potential Enablers of Human Autonomy in IoT

From your perspective, what do you believe to be the most critical factors that could enable human autonomy in the future of IoT?

Please explain your reasoning. Kindly answer this question before proceeding to the next segment.

In this section, factors that can be enablers towards more human autonomy in IoT are introduced. You will be asked to indicate your level of agreement on whether the particular factors enable human autonomy. By enabling human autonomy, we mean anything that enhances or preserves human agency, human empowerment, or human control, in IoT.

Rate the following statements on a scale of 1 to 7, where 1 represents “Strongly Disagree” and 7 represents “Strongly Agree”.

Please consider whether the factors are potential enablers towards achieving human autonomy in IoT.

	1: Strongly disagree	2: Disagree	3: Somewhat disagree	4: Neutral	5: Somewhat agree	6: Agree	7: Strongly agree	I don't know
Allowing users to customize machine-to-machine automation between IoT devices, i.e., by the use of End User Development methods. *	○	○	○	○	○	○	○	○
Personalized privacy recommendations for data sharing and processing in IoT. *	○	○	○	○	○	○	○	○
Transparency and explainability of IoT systems, allowing users to understand how their data is collected, processed, and used. *	○	○	○	○	○	○	○	○
Accessibility for users with impairments, i.e., a configurable user interface that presents different levels of interaction corresponding to the levels of a user's abilities. *	○	○	○	○	○	○	○	○
Designing privacy policies that are easy to understand. *	○	○	○	○	○	○	○	○
The use of frameworks such as privacy-by-design and value-sensitive design when developing IoT systems. *	○	○	○	○	○	○	○	○
System sends nudges or notifications that warn users of risk-averse situations, i.e., when they are about to share personal data. *	○	○	○	○	○	○	○	○
Providing innovative interaction strategies for human-to-machine communication, i.e., voice command, user-friendly interfaces. *	○	○	○	○	○	○	○	○
Improved information security and communication network security. *	○	○	○	○	○	○	○	○
Clear conveyance of accountability in complex IoT systems and systems-of-systems. *	○	○	○	○	○	○	○	○

Nettskjema

Importance of enablers for future IoT

You will now be asked to indicate how important you believe the previously mentioned factors are for enabling human autonomy in future design and use of IoT. Please read Scenario 1 and rate the statements below accordingly.

Scenario 1: By 2035, smart environments and IoT will allow humans to retain full agency over IoT systems, enjoying the benefits of automation, connectivity, and efficiency while maintaining control over their own lives.

To what extent to you think the following factors are important in contributing towards Scenario 1 becoming a reality?

Please read the statements listed below. Rate the statements on a scale of 1 to 7, where 1 represents "Not important at all" and 7 represents "Very important".

	1: Not at all important	2: Low importance	3: Slightly important	4: Neutral	5: Moderately important	6: Very important	7: Extremely important	I don't know
Allowing users to customize machine-to-machine automation between IoT devices, i.e., by the use of End User Development methods. *	○	○	○	○	○	○	○	○
Personalized privacy recommendations for data sharing and processing in IoT. *	○	○	○	○	○	○	○	○
Transparency and explainability of IoT systems, allowing users to understand how their data is collected, processed, and used. *	○	○	○	○	○	○	○	○
Accessibility for users with impairments, i.e., a configurable user interface that presents different levels of interaction corresponding to the levels of a user's abilities. *	○	○	○	○	○	○	○	○
Designing privacy policies that are easy to understand. *	○	○	○	○	○	○	○	○
Regulations and legal directives such as GDPR. *	○	○	○	○	○	○	○	○
The use of frameworks such as privacy-by-design and value-sensitive design when developing IoT systems. *	○	○	○	○	○	○	○	○
System sends nudges or notifications that warn users of risk-averse situations, i.e., when they are about to share personal data. *	○	○	○	○	○	○	○	○

Providing innovative interaction strategies for human-to-machine communication, i.e., voice command, user-friendly interfaces. *	○	○	○	○	○	○	○	○
Improved information security and communication network security. *	○	○	○	○	○	○	○	○
Clear conveyance of accountability in complex IoT systems and systems-of-systems. *	○	○	○	○	○	○	○	○

If applicable, please explain why you gave this answer:

How likely do you consider it to be that Scenario 1 becomes a reality? *

- □ Very likely
- □ Likely
- □ Neutral
- □ Unlikely
- □ Very unlikely

Regardless of viability, how desirable do you find Scenario 1 to be? *

- □ Very desirable
- □ Desirable
- □ Neutral
- □ Undesirable
- □ Very undesirable

Section: Potential Barriers to Human Autonomy

From your perspective, please describe potential barriers against human autonomy in IoT.

Please provide specific examples or scenarios and explain your reasoning. Kindly answer this question before proceeding to the next segment.

Nettskjema

In this section factors that can be barriers against more human autonomy in IoT are introduced. You will be asked to indicate your level of agreement on whether the particular factors inhibit human autonomy. By inhibiting human autonomy, we mean anything that impairs or inhibits human agency, human empowerment, or human control, in IoT.

Rate the following statements on a scale of 1 to 7, where 1 represents “Strongly Disagree” and 7 represents “Strongly Agree”.

Please consider whether the factors are potential barriers to achieving human autonomy in IoT.

	1: Strongly disagree	2: Disagree	3: Somewhat disagree	4: Neutral	5: Somewhat agree	6: Agree	7: Strongly agree	I don't know
Third-party interest in gathering information from personal intelligent environments (surveillance). *	○	○	○	○	○	○	○	○
Third-party interest in seeking control over personal environments. *	○	○	○	○	○	○	○	○
Lack or concealment of user configuration capabilities in IoT devices. *	○	○	○	○	○	○	○	○
Limitations in configurability of IoT, restricting the user’s options to predetermined pathways created by programmers. *	○	○	○	○	○	○	○	○
ICT developers not recognizing the need for variations in development of IoT devices. *	○	○	○	○	○	○	○	○
Dependence on centralized authorities and service providers, potentially leading to data monopolies. *	○	○	○	○	○	○	○	○
The speed of the evolution of IoT is outpacing regulatory processes, potentially impairing effectiveness of regulations. *	○	○	○	○	○	○	○	○
Limited support for ensuring informed consent in IoT, i.e., giving users the opportunity to accept or oppose data collection and use. *	○	○	○	○	○	○	○	○
Systemic biases, i.e., in business models, market competition, regulatory frameworks or any other aspects regarding the operational delivery of services. *	○	○	○	○	○	○	○	○
Users do not have complete information about consequences of disclosing data, i.e., systems’ collection of position data. *	○	○	○	○	○	○	○	○

The Digital Divide – unequal access to technology (such as IoT) in society, potentially disadvantaging part of the population. *	○	○	○	○	○	○	○	○

Importance of barriers for future IoT

You will now be asked to indicate how important the previously mentioned aspects are for hindering human autonomy in future design and use of IoT. Please read Scenario 2 and rate the statements below accordingly.

Scenario 2: By 2035, smart environments and IoT will be built in a way so that humans lose agency, resulting in a loss of personal freedom, diminished privacy, and control over one's life.

To what extent to you think the following factors are important in contributing towards Scenario 2 becoming a reality?

Please read the statements listed below. Rate the statements on a scale of 1 to 7, where 1 represents "Not important at all" and 7 represents "Very important".

	1: Not at all important	2: Low importance	3: Slightly important	3: Neutral	4: Moderately important	6: Very important	6: Extremely important	I don't know
Third-party interest in gathering information from personal intelligent environments (surveillance). *	○	○	○	○	○	○	○	○
Third-party interest in seeking control over personal environments. *	○	○	○	○	○	○	○	○
Lack or concealment of user configuration capabilities in IoT devices. *	○	○	○	○	○	○	○	○
Limitations in configurability of IoT, restricting the user's options to predetermined pathways created by programmers. *	○	○	○	○	○	○	○	○
ICT developers not recognizing the need for variations in development of IoT devices. *	○	○	○	○	○	○	○	○
Dependence on centralized authorities and service providers, potentially leading to data monopolies. *	○	○	○	○	○	○	○	○
The speed of the evolution of IoT is outpacing regulatory processes, potentially impairing effectiveness of regulations. *	○	○	○	○	○	○	○	○
Limited support for ensuring informed consent in IoT, i.e., giving users the opportunity to accept or oppose data collection and use. *	○	○	○	○	○	○	○	○

Systemic biases, i.e., in business models, market competition, regulatory frameworks or any other aspects regarding the operational delivery of services. *	○	○	○	○	○	○	○	○
Users do not have complete information about consequences of disclosing data, i.e., systems' collection of position data. *	○	○	○	○	○	○	○	○
The Digital Divide – unequal access to technology (such as IoT) in society, potentially disadvantaging part of the population. *	○	○	○	○	○	○	○	○

If applicable, please explain why you gave this answer:

How likely do you consider it to be that Scenario 2 becomes a reality? *

- □ Very likely
- □ Likely
- □ Neutral
- □ Unlikely
- □ Very unlikely

Regardless of viability, how desirable do you find Scenario 2 to be? *

- □ Very desirable
- □ Desirable
- □ Neutral
- □ Undesirable
- □ Very undesirable

Are there any other factors, enablers, or barriers related to human autonomy in IoT that you think should be considered in this study? Please elaborate.

Appendix F
End-user Survey

The subsequent pages contain the questionnaire that was used in the end-user survey. In the multiple choice questions, the checkboxes represent mutually exclusive answer options.

Survey: How to preserve human autonomy for future smart technology-based experiences

Mandatory fields are marked with a star *

This survey is a part of a study exploring aspects that influence human autonomy in the Internet of Things (IoT). If you are not familiar with IoT (or human autonomy), don't worry! Relevant terms and concepts will be explained.

The survey is divided into five parts:

1. Demographics
2. Familiarity with intelligent environment technology and IoT
3. Your interpretation of the term 'human autonomy'
4. Potential enablers of human autonomy
5. Potential barriers to human autonomy

It takes around **10 minutes** to fill out the survey. All information will be treated confidentially. The technical implementation of the survey is done in Nettskjema and the data are gathered completely anonymously.

If you have any questions or comments related to the survey, contact Silje Kløften Lein (siljkle@stud.ntnu.no), master's student in communication technology at the Norwegian University of Science and Technology (NTNU).

P.P.S: I am also looking for experts with a bit more knowledge on the topic of smart environments to participate in an expert survey. If you know of someone or consider yourself to be one, please email me on siljkle@stud.ntnu.no for more information.

Section: Demographics

Please specify your gender. *

□ Female
□ Male
□ Non-binary
□ Other
□ Prefer not to say

Which age group do you belong to? *

Please select the option that best represents your age range.

□ 18-24
□ 25-34
□ 35-44
□ 45-54
□ 55-64
□ 65 or above
□ Prefer not to say

Where are you located? *
Please indicate your permanent residence.

- □ Norway
- □ Europe (outside of Norway)
- □ North America
- □ Africa
- □ South America
- □ Asia
- □ Australia
- □ Other

What is the highest level of education you have completed? *
Please select the option that best describes your educational background. If you are currently enrolled in a study program, please select the level of the degree you are enrolled in (i.e., if you are a master's student, select 'Master's degree').

- □ Upper Secondary School/High School Diploma
- □ Bachelor’s Degree
- □ Master’s Degree
- □ Doctorate/Ph.D
- □ Other

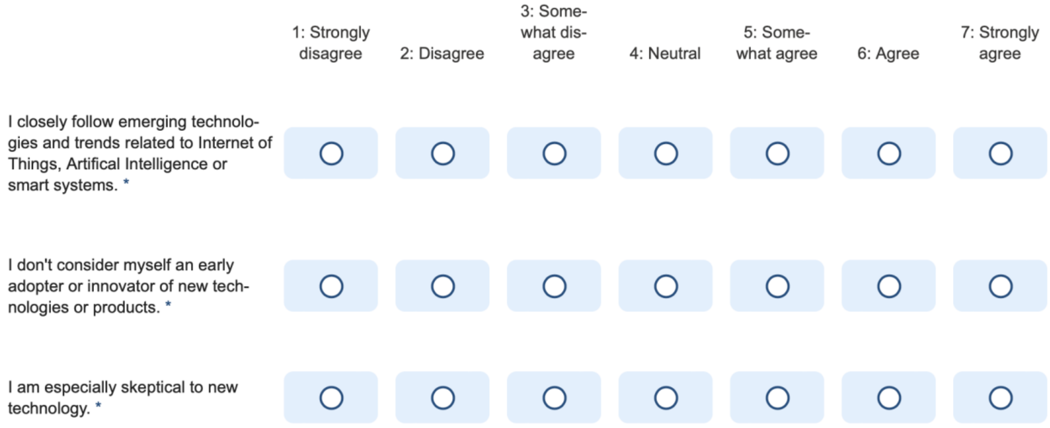
What is your current occupation? *
Please select the option that best represents your situation.

- □ Student
- □ Manual labor
- □ Executive/management
- □ Self-employed
- □ Employed in a public or private sector
- □ Unemployed/job seeker
- □ Unable to work
- □ Retired
- □ Other

Section: Familiarity with the Internet of Things (IoT)

Rate your level of agreement with the following statements on a scale of 1 to 7, where 1 represents “Strongly Disagree” and 7 represents “Strongly Agree”.

Explanation of concepts:
The Internet of Things (IoT) connects everyday objects to the internet, letting them communicate and share information with users and other devices. Examples are smart thermostats that can adjust the temperature automatically, smart refrigerators that can notify the user when they are running low on groceries, and smart security systems that can send an alert to the user if it detects suspicious activity. An intelligent environment consists of several IoT devices connected together.
Early adopters are those individuals that use new products before the majority of people. They are often among the first to try out and adopt new gadgets, software, or services.



	1: Strongly disagree	2: Disagree	3: Somewhat disagree	4: Neutral	5: Somewhat agree	6: Agree	7: Strongly agree
I closely follow emerging technologies and trends related to Internet of Things, Artifical Intelligence or smart systems. *	○	○	○	○	○	○	○
I don't consider myself an early adopter or innovator of new technologies or products. *	○	○	○	○	○	○	○
I am especially skeptical to new technology. *	○	○	○	○	○	○	○

Section: Your interpretation of “human autonomy”

The term 'human autonomy' is described with different definitions in literature. This research aims to map the correspondence between definitions from literature and people's perception of the term. If the definitions listed below differ from your view you are given the chance to describe it in your own words. You also have the option to indicate that you are not familiar with the term.

What does the term 'human autonomy' mean to you in the context of everyday life? *
Select the option that best describes your view. There is no right or wrong answer to this question, we are interested in your perception of the term.

□ My ability to make choices and decisions freely, without being restricted or dictated by others or technology.

□ Feeling empowered to determine my own path and live according to my values and preferences.

□ My ability to be in control of my life and my actions.

□ I don’t know

□ Other

If you chose 'Other', please specify:
This element is only shown when the option ‘Other’ is selected in the question ‘What does the term 'human autonomy' mean to you in the context of everyday life?’

What does the term 'human autonomy' mean to you in the technical context of intelligent environments? I.e., smart home, smart surveillance, smart thermostat.
Please select the option that best fits according to your view. There is no right or wrong answer to this question, we are interested in your perception of the term.

□ My ability to make choices and decisions freely, without being restricted or dictated by others or technology.

□ Feeling empowered to determine my own path and live according to my values and preferences, even in the presence of advanced technologies like the Internet of Things.

□ My ability to control the system and the information I share with it.

□ I don’t know

□ Other

If you chose 'Other', please specify:

This element is only shown when the option ‘Other’ is selected in the question ‘What does the term 'human autonomy' mean to you in the technical context of intelligent environments? I.e., smart home, smart surveillance, smart thermostat.’

Section: Potential Enablers of Human Autonomy in IoT

In the following section we will use terms with definitions as described below:

The Internet of Things (IoT) connects everyday objects to the internet, letting them communicate and share information with users and other devices. Examples are smart thermostats that can adjust the temperature automatically, smart refrigerators that can notify the user when they are running low on groceries, and smart security systems that can send an alert to the user if it detects suspicious activity.

An intelligent environment consists of several IoT devices connected together.

Human autonomy can be defined as self-governance or self-determination, maintaining control over one's own life, acheiving individual goals and making one's own choices.

Rate the following statements on a scale of 1 to 7, where 1 represents “Strongly Disagree” and 7 represents “Strongly Agree”.

Please consider the following statements, and indicate your level of agreement to whether the aspects enable people to have autonomy and control over their own actions and decisions in an IoT context.

	1: Strongly disagree	2: Disagree	3: Somewhat disagree	4: Neutral	5: Somewhat agree	6: Agree	7: Strongly agree	I don't know
Letting people adapt to their specific needs how smart devices (i.e., smart watch and mobile phone) interact with each other in a way that doesn’t require technical expertise. *	○	○	○	○	○	○	○	○
Providing personalized suggestions on how to keep information private when sharing and using data with smart devices connected to the Internet of Things. *	○	○	○	○	○	○	○	○
Making sure that smart devices are open and clear about how they collect, process, and use your information, so users can understand what happens with their data. *	○	○	○	○	○	○	○	○

Nettskjema

Accessibility to smart devices for users with impairments, such a configurable user interface that can be adjusted according to the levels of a user's abilities. *	○	○	○	○	○	○	○	○
Designing privacy policies (i.e., at specific device or service level) that are easy to understand. *	○	○	○	○	○	○	○	○
Regulations and legal frameworks (i.e., GDPR) that have implications for which types of personal data can be gathered about users, how the data can be used, etc. *	○	○	○	○	○	○	○	○
Principles for developing IoT systems in an ethical and responsible way, i.e., IoT developers considering and prioritizing privacy and ethics from the beginning of development. *	○	○	○	○	○	○	○	○
The system sends messages or notifications to warn users when they might be sharing personal data that could be risky, i.e., an alert that pops up when the user is about to share sensitive data. *	○	○	○	○	○	○	○	○
Offering new and creative ways for people to communicate with machines, such as using voice commands or easy-to-use interfaces when interacting with smart devices. *	○	○	○	○	○	○	○	○
Improving the protection of information and making sure that communication networks are secure from potential threats or unauthorized access. *	○	○	○	○	○	○	○	○
Ensuring that responsibility is clearly assigned and understood among different parties in complex IoT systems and networks of interconnected systems. *	○	○	○	○	○	○	○	○

Which aspects do you think are the most important for enabling people to have control over their own decisions and actions in the future of Internet of Things (IoT)?

Please explain why you think these aspects are critical. You can also describe aspects that are not listed above.

Importance of enablers for future IoT

You will now be asked to indicate how important you believe the previously mentioned factors are for enabling human autonomy in future design and use of IoT. Please read Scenario 1 and rate the statements below accordingly.

Scenario 1: By 2035, smart environments and IoT will allow humans to retain full agency over IoT systems, enjoying the benefits of automation, connectivity, and efficiency while maintaining control over their own lives.

To what extent to you think the following factors are important in contributing towards Scenario 1 becoming a reality?

Please read the statements listed below. Rate the statements on a scale of 1 to 7, where 1 represents "Not important at all" and 7 represents "Very important".

	1: Not at all important	2: Low importance	3: Slightly important	4: Neutral	5: Moderately important	6: Very important	7: Extremely important	I don't know
Letting people adapt to their specific needs how smart devices (i.e., smart watch and mobile phone) interact with each other in a way that doesn't require technical expertise. *	○	○	○	○	○	○	○	○
Providing personalized suggestions on how to keep information private when sharing and using data with smart devices connected to the Internet of Things. *	○	○	○	○	○	○	○	○
Making sure that smart devices are open and clear about how they collect, process, and use your information, so users can understand what happens with their data. *	○	○	○	○	○	○	○	○
Accessibility to smart devices for users with impairments, such a configurable user interface that can be adjusted according to the levels of a user's abilities. *	○	○	○	○	○	○	○	○
Designing privacy policies (i.e., at specific device or service level) that are easy to understand. *	○	○	○	○	○	○	○	○
Regulations and legal frameworks (i.e., GDPR) that have implications for which types of personal data can be gathered about users, how the data can be used, etc. *	○	○	○	○	○	○	○	○
Principles for developing IoT systems in an ethical and responsible way, i.e., IoT developers considering and prioritizing privacy and ethics from the beginning of development. *	○	○	○	○	○	○	○	○

The system sends messages or notifications to warn users when they might be sharing personal data that could be risky, i.e., an alert that pops up when the user is about to share sensitive data. *	○	○	○	○	○	○	○	○
Offering new and creative ways for people to communicate with machines, such as using voice commands or easy-to-use interfaces when interacting with smart devices. *	○	○	○	○	○	○	○	○
Improving the protection of information and making sure that communication networks are secure from potential threats or unauthorized access. *	○	○	○	○	○	○	○	○
Ensuring that responsibility is clearly assigned and understood among different parties in complex IoT systems and networks of interconnected systems. *	○	○	○	○	○	○	○	○

Section: Potential Barriers to Human Autonomy in IoT

In the following section we will use terms with definitions as described below:
The Internet of Things (IoT) connects everyday objects to the internet, letting them communicate and share information with users and other devices. Examples are smart thermostats that can adjust the temperature automatically, smart refrigerators that can notify the user when they are running low on groceries, and smart security systems that can send an alert to the user if it detects suspicious activity. An intelligent environment consists of several IoT devices connected together.
Human autonomy can be defined as self-governance or self-determination, maintaining control over one's own life, acheiving individual goals and making one's own choices.

Rate the following statements on a scale of 1 to 7, where 1 represents "Strongly Disagree" and 7 represents "Strongly Agree".

Please consider the following statements, and indicate your level of agreement to whether the aspects hinder people of having autonomy and control over their own actions and decisions in an IoT context.

	1: Strongly disagree	2: Disagree	3: Somewhat disagree	4: Neutral	5: Somewhat agree	6: Agree	7: Strongly agree	I don't know
Third-party interest in gathering information from personal intelligent environments (surveillance). *	○	○	○	○	○	○	○	○
Third-party interest in seeking control over personal environments. *	○	○	○	○	○	○	○	○
User configuration capabilities and settings in smart devices being hidden or hard to find. *	○	○	○	○	○	○	○	○

Smart devices limiting the user’s control options to specific pathways programmed by the developers. *	○	○	○	○	○	○	○	○
ICT developers not recognizing the need for variations in development of smart devices. *	○	○	○	○	○	○	○	○
Dependence on a few powerful organizations or companies that control important services and data, which can result in a situation where they have a lot of control over IoT user information, like a monopoly. *	○	○	○	○	○	○	○	○
The Internet of Things (IoT) is developing very quickly, but the rules and regulations to govern it are not keeping up, possibly making it harder for regulations to work well and do their job effectively. *	○	○	○	○	○	○	○	○
Limited support for ensuring informed consent in IoT, i.e., giving users the opportunity to accept or oppose data collection and use. *	○	○	○	○	○	○	○	○
Systemic biases/unfairness existing within how services are provided. I.e., biases in how businesses operate, compete in the market, or how regulations are set up. *	○	○	○	○	○	○	○	○
Users may not have all the information they need to understand what might happen when they share their data, i.e., when systems collect information about their location. *	○	○	○	○	○	○	○	○
The Digital Divide – unequal access to technology (such as IoT) in society, potentially disadvantaging part of the population. *	○	○	○	○	○	○	○	○

In your opinion, what are the major challenges that need to be addressed to make sure that humans have control over own decisions and actions in the IoT ecosystem?

Please explain why you think these aspects are critical. You can also describe challenges that are not listed above.

Nettskjema

Importance of barriers for future IoT

You will now be asked to indicate how important the previously mentioned aspects are for hindering human autonomy in future design and use of IoT. Please read Scenario 2 and rate the statements below accordingly.

Scenario 2: By 2035, smart environments and IoT will be built in a way so that humans lose agency, resulting in a loss of personal freedom, diminished privacy, and control over one's life.

To what extent to you think the following factors are important in contributing towards Scenario 2 becoming a reality?

Please read the statements listed below. Rate the statements on a scale of 1 to 7, where 1 represents "Not important at all" and 7 represents "Very important".

	1: Not important at all	2: Low importance	3: Slightly important	4: Neutral	5: Moderately important	6: Very important	7: Extremely important	I don't know
Third-party interest in gathering information from personal intelligent environments (surveillance). *	○	○	○	○	○	○	○	○
Third-party interest in seeking control over personal environments. *	○	○	○	○	○	○	○	○
User configuration capabilities and settings in smart devices being hidden or hard to find. *	○	○	○	○	○	○	○	○
Smart devices limiting the user's control options to specific pathways programmed by the developers. *	○	○	○	○	○	○	○	○
ICT developers not recognizing the need for variations in development of smart devices. *	○	○	○	○	○	○	○	○
Dependence on a few powerful organizations or companies that control important services and data, which can result in a situation where they have a lot of control over IoT user information, like a monopoly. *	○	○	○	○	○	○	○	○
The Internet of Things (IoT) is developing very quickly, but the rules and regulations to govern it are not keeping up, possibly making it harder for regulations to work well and do their job effectively. *	○	○	○	○	○	○	○	○
Limited support for ensuring informed consent in IoT, i.e., giving users the opportunity to accept or oppose data collection and use. *	○	○	○	○	○	○	○	○

Systemic biases/unfairness existing within how services are provided. I.e., biases in how businesses operate, compete in the market, or how regulations are set up. *	○	○	○	○	○	○	○	○
Users may not have all the information they need to understand what might happen when they share their data, i.e., when systems collect information about their location. *	○	○	○	○	○	○	○	○
The Digital Divide – unequal access to technology (such as IoT) in society, potentially disadvantaging part of the population. *	○	○	○	○	○	○	○	○

Do you have anything to add or any final comments related to this survey or the topic?

Generated: 2023-07-16 19:19:50.

Appendix G
Literature Review Coding Scheme

The Excel coding scheme from the systematic literature review is not included in the appendix as it is an extensive file with a number of columns and rows, which would take up a considerable amount of space. It would also have required significant editing to transfer all the information from the spreadsheet, which was not prioritized due to time and resource constraints. However it is possible to ask to view the complete Excel file with all the articles coded.

NTNU

Norwegian University of
Science and Technology