Foresight Scenarios for Protecting Human Autonomy in IoT: A Comparative Study of Expert and End-User Perspectives

Kaja Fjørtoft Ystgaard
kaja.ystgaard@ntnu.no
NTNU — Norwegian University of Science and Technology, Norway

Silje Kløften Lein
NTNU — Norwegian University of Science and Technology, Norway

Katrien De Moor
katrien.demoor@ntnu.no
NTNU — Norwegian University of Science and Technology, Norway

ABSTRACT

This article presents a comparative study, from a multi-stakeholder perspective, aimed at defining future scenarios that safeguard human autonomy in the context of IoT technologies. The research utilizes a systematic literature review (n=40) to identify factors that protect or undermine human autonomy in IoT, followed by two quantitative surveys using Delphi elements to compare expert (n=12) and end-user (n=123) perspectives. The paper sheds light on areas of consensus and divergence in understanding human autonomy and identifies key factors that contribute to optimistic and pessimistic scenarios. The findings offer valuable insights for future scenario development and policy formulation to ensure the responsible deployment of IoT technologies.

CCS CONCEPTS

• **Security and privacy** → **Human and societal aspects of security and privacy**; *Social aspects of security and privacy*; • **Computer systems organization** → *Sensor networks*; • **Human-centered computing** → *HCI theory, concepts and models.*

KEYWORDS

Human-Centered Research, Internet of Things, Human Autonomy, Delphi, Scenario Assessment

ACM Reference Format:
Kaja Fjørtoft Ystgaard, Silje Kløften Lein, and Katrien De Moor. 2023. Foresight Scenarios for Protecting Human Autonomy in IoT: A Comparative Study of Expert and End-User Perspectives. In *The International Conference on the Internet of Things (IoT 2023), November 07–10, 2023, Nagoya, Japan.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3627050.3627061

1 INTRODUCTION

The rapid evolution of the Internet of Things (IoT) and intelligent networks have brought significant changes to the role of humans in future technological developments [3]. As IoT technologies are becoming more pervasive and intelligent fueled by recent advances in Artificial Intelligence (AI); there is growing concern about their potential impact on human autonomy [20, 28]. In reaction to these developments, immediate and future human-centered policies and legal frameworks have brought forward several well-intended design visions and ambitions, in which humans' autonomy and ability to participate as free agents have been prioritized in the technical design [14, 32, 42]. Nevertheless, to have IoT technical contributions that can achieve fair and trustworthy outcomes [34], the power gap between those who are deploying vs. those subjected to the technology needs closing instead of widening [8]. Further, existing issues are mostly related to how people can trust the interaction with automated intelligent environments by configuring in the protection of human/user rights [39], in particular of meaningful human autonomy [40]. By designing for meaningful autonomy, as a fundamental psychological need and component of well-being [9], humans' ability to influence and control personal and public environments is accounted for [20].

Currently, the human-centric design aiming to address these issues in the context of IoT and sensor networks primarily focuses on human well-being, human privacy, security, control, and end-user participation [42]. In the technical translation, most IoT sensing and interaction functionalities come with human-centric features that use AI and machine learning to achieve "human-like" [16, 29] or ethical abilities [5], and more transparent/accessible/easy-to-use human-environment interfaces [38]. However, despite this human-centric rationale, there are challenges related to establishing a clear link between more human-centered outcomes and the corresponding technology manifestation [42], partly due to needing more shared guidelines and design frameworks geared towards technical domains [15].

The prime objective of this research is to define future scenarios that can tackle challenges related to the undermining/threatening (as undesired outcome) or promoting (as desired outcome) human autonomy in IoT. A part of the overall research scope is to assess which future developments/factors can bring forth technical solutions that safeguard human autonomy in IoT. In this research, a particular focus is therefore put on the identification of key factors contributing to optimistic and pessimistic scenarios of human autonomy protection and mapping future areas of consensus and divergence between experts and end-users (as often overlooked, yet key stakeholders) in understanding human autonomy. This approach is motivated by the assumption that defining scenarios where there is consensus, can help to better understand where IoT technical frameworks may fail in the future or where a human-centered theoretical approach can help to orient the design towards the envisioned human-empowering outcomes [27]. An additional assumption is that the existing technical solutions in IoT do not account for the human agency that goes lost [26], for those impacted by it, and for the negative outcomes it triggers [33].

The following research questions guided our work:

IoT 2023, November 07–10, 2023, Nagoya, Japan

ACM ISBN 979-8-4007-0854-1/23/11.
https://doi.org/10.1145/3627050.3627061

- RQ1 What are the existing and future developments/factors that protect (positive influence) or undermine (negative influence) human autonomy in the context of IoT technologies?
- RQ2 What are the theoretical and conceptual interpretations of human autonomy, and how are they operationalised into technical IoT frameworks? Do the interpretations of the concept of human autonomy by experts and end-users differ and if so, in which ways?
- RQ3 What are the perceptions of experts and end-users regarding the developments and factors that hold the most significant potential impact on future scenarios concerning human autonomy preservation or loss?

To address these questions, we first conducted a systematic literature review (SLR) to identify the existing developments/factors that *currently* impact human autonomy within IoT systems. Building upon the SLR analysis (n=40), we aimed to investigate the broader understanding of human autonomy, as well as potential *future* developments/factors, using a participatory Foresight approach. To this end, we conducted two delphi method-inspired quantitative surveys, one targeting experts (n=12) and one targeting end-users (n=123). The rest of this paper is organized as follows: Section 2 provides relevant background and is followed by Section 3, which describes the overall research approach and operationalization of the studies. The key results are presented in Section 4 and further discussed in Section 5. Finally, Section 6 concludes the paper.

2 BACKGROUND

2.1 Context and challenges to human autonomy

Human-centric IoT functionalities play a central role in allowing humans to control and interact with the IoT system, influencing the decisions made by these sensing technologies [35]. While what is referred to as human-centric IoT can be associated with both positive outcomes (e.g., human empowerment), there is also a manifestation of negative potentials (e.g., invasive surveillance and persuasion/coercion) [28] that cannot be overlooked. On the one hand, technical developments in IoT that aim to genuinely protect human autonomy target similar non-instrumental outcomes, such as the human agency, empowerment, and control [9, 32]. On the other hand, an important observation is that the power of the underlying technology seems to be growing [19]. For instance, recent advances in human-centric IoT functionalities incorporate personalised and user/socially-aware intelligence into the sensing environment, while the increased surveillance, intelligence, and automated decisioning grants more control, visibility/power, and agency to the networked machines [3].

The existing human-centric technical functionalities in IoT are currently addressed by introducing human-centric features aimed at adapting to specific and dynamic user needs and achieve "smooth experiences" [37]. In this view, human-centric IoT refers to a connected network of sensors, objects, and machines with more "humanlike" capacities and behaviors, e.g., based on context-aware, user-aware, social-aware [12], and participatory sensing technology [25]. These user- or social-aware mechanisms allow continuous monitoring of the user to enable networked environments to adapt automatically to the desired or predicted user needs [6, 12].

More recently, an introduction of human-centric technical interfaces is looking to provide meaningful human autonomy and sovereignty, also in the networking context [17]. Such mechanisms aiming to safeguard human autonomy, intend to keep humans actively involved on their own terms [40], and in other words, can provide meaningful human involvement or control [35]. Furthermore, in such approaches, the system includes human input in the process, method, technique, or solution to protect human performance [43]. In this regard, interfaces that let humans observe / interact with the IoT system aim to provide transparency, understandability, and accountability features to help humans monitor and interact with persuasive IoT technology [38]. However, providing meaningful involvement and autonomy requires early involvement of users and other stakeholders [43]. However, it can be questioned whether the traditional evaluation approaches ([25]) allow to reach the intended outcomes. The latter requires that human and society's genuine interests are systematically considered and that the design is oriented towards a public-good design logic [41].

2.2 Human autonomy and IoT: future scenarios

To realize the above-mentioned ambitions, namely to build a future IoT ecosystem that is democratic, trustworthy, and fair, the human-centered design objectives, and how they are technically operationalised, will need to factor in for whom, when, and how these technologies are dis-empowering (e.g., reducing autonomy) and empowering [20, 31]. Consequently, the involvement of multiple stakeholders and disciplinary perspectives in the human-centric IoT design process is required. However, to date, there is still a gap in the literature regarding incorporating human-centered theories that account for alternative, social, and multi-disciplinary design paradigms in the field of IoT [43]. Examples include situated [1], critical [30], or socially constructed analyses [7] of the underlying power dynamics of the technical design. Adopting theories that bring in such more critical perspectives, can allow for future technical developments that are genuinely able to configure *and* safeguard human autonomy in IoT, by also ensuring that human users' have the ability to influence, or resist the technical system [43].

We identified three simplified categories of theoretical assumptions/foundations in the literature, that could be used for situating human-centric translations in IoT. One is "*rational*", with the pursuit of pre-determined technical problems and their closure [23]. The second one is "*humanistic*", where the exploration involves alternative designs aiming to be beneficial to humans and society [4]. A part of the humanistic technical paradigms can account for technology as "situated", "socially constructive", and "subjective". Finally, the third category is a "*judiciary*" framework that strictly follows legal guidelines [4]. In this respect, the underlying theoretical assumptions implicate the real-world consequences of the loss of human and societal agency in next-generation IoT technology developments [30]. Examining IoT developments and future directions from multiple perspectives, in a manner that is sensitive to the role, assumptions and intent of the designers therefore can allow to identify underlying subjective interpretations and power dynamics of specific IoT solutions [4]. Further, future intelligent networks rely on autonomous and perceptive functionalities, which will directly impact people's lives [36]. However, existing studies

indicate important discrepancies between different stakeholders in terms of e.g., future developments and how much control such pervasive and intelligent functionalities should be given [44] and on the role of human autonomy in future autonomous systems [2]. While the involvement of experts in such future-oriented analyses is common, end-users seemingly have had less prominence in influencing the future IoT technical developments in the assessment of the role of human agency. We address this lack in this work, as will be explained in Section 3.

Secondly, to manage the user-technology negotiation also from a more forward-looking perspective, the value of proactively or re-actively addressing failures has recently been underlined in the literature [27]. In response to evolving regulatory demands that necessitate readjustment, there is a growing recognition of the importance of anticipating and addressing failures, within the ambit of technology design [10, 13]. As such, it makes sense to envision future scenarios in either negative or positive terms, where the most negative developments potentially lead to diminished or even the total loss of human agency entirely to the advantage of intelligent automated networks [2]. Given the need to assess both an optimistic vs. a pessimistic future design scenario, from multiple perspectives, a participatory Foresight-based methodological approach was adopted in this research.

3 METHODOLOGY

First, to address RQ1, we conducted a systematic literature review (n=40) to map the existing and potential future factors that may shape the preservation or erosion of human autonomy in IoT. Secondly, we conducted two surveys to compare experts' (n=12) with end-users' (n=123) perspectives on these developments, in order to answer RQ2, assessing interpretations of human autonomy, and RQ3, assessing the importance and expected impact/contribution of the identified developments towards a positive and negative future scenario.

3.1 Systematic literature review

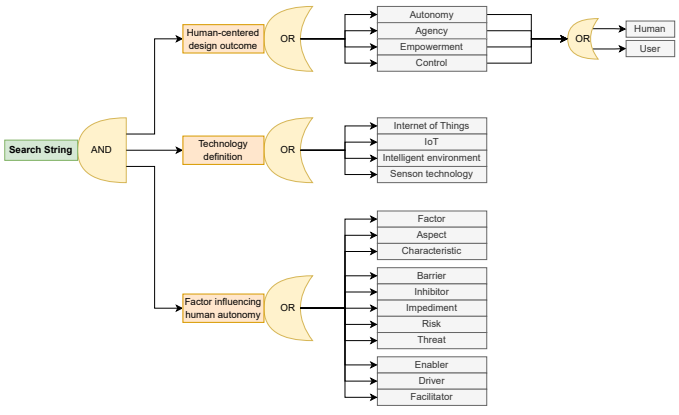

Figure 1: Logic diagram of the search string used for the keyword search.

The main goal with the systematic literature review (SLR) was to identify and analyze factors that impact human autonomy. Following the framework of [21], the three most important phases of the SLR method consist of 1) The input stage, 2) The processing stage and 3) The output stage.

The input stage involved a targeted search strategy. The keywords were selected from relevant literature, and focused on design outcomes, technical definitions, and factors that influence the future technical trajectory. After three rounds of iterations, the keyword strategy and search string illustrated in Figure 1 was selected. The first category targeted human-centered design outcomes related to human autonomy, including variations of the term (agency, empowerment, control) and having a focus on recognizing and supporting the autonomy of individuals while maintaining control over their environment [18]. 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 related to IoT. Lastly, the third category consists of synonyms for factors influencing human autonomy in IoT to determine both positive and negative development paths. While there is a vast amount of articles on these branches individually, we aimed to capture only literature combining them, thus strongly limiting the output.

To facilitate the processing stage, a comprehensive selection protocol was devised in advance. Peer-reviewed academic literature discussing the definition of human autonomy and/or technical and non-technical factors within the technical IoT context, was considered for inclusion. Literature was excluded if it only superficially referred to human autonomy or the aforementioned related terms, or if the work was solely oriented towards business or technology.

The search included several multi-disciplinary scientific databases, namely Web of Science, Scopus, IEEE and ACM Digital Library. 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. After eliminating duplicate entries, a detailed screening process of titles, abstracts and keywords, based on the selection criteria, further narrowed down the selection to 46 articles. After a thorough assessment of the full texts, six articles that failed to meet the criteria were excluded. As a result, the final count stood at 40 articles.

Each article was manually coded after reading and interpreting every article, according to the variables/themes and corresponding categories summarized in Table 1. In addition, the statistical software program SPSS was used to perform simple statistical analyses of the general characteristics of the dataset.

3.2 Expert and end-user surveys

Rationale. Two quantitative surveys, one targeting experts and one consumers, were designed applying elements of the Delphi method [22]. The design allowed for evaluating the factors identified in previous studies from existing literature (captured by means of the SLR) and for comparing the expected future impact. The Delphi method is an approach within the Foresight discipline [24], which seeks judgement from experts on a topic [22]. It facilitates gaining consensus among experts and stakeholders from different perspectives. The method entails administrating surveys to capture

Table 1: Themes each article was sorted according to in the Excel coding scheme.

Theme	Explanation
Title	Title of the article.
Author	Author(s) of the article.
Geography	Location of research institution(s).
Perspective	Multidisciplinary or single discipline.
Expertise	Field of research of the author(s).
Design outcome	Human-centered design outcome (e.g., autonomy, empowerment, control, privacy).
Theory	Theories for design, or other theories underlying the presented work.
Framework	Design framework (Design principles guiding the development of technical IoT solutions).
Factor	Aspect influencing human autonomy in IoT.
Future research	Identified research gaps.
Technical solution	Specified technical solution to achieve human-centered outcomes in IoT.

expert knowledge and can be particularly useful in investigating topics characterized by substantial uncertainty about the future and future situations [24]. While a full, iterative Delphi was not possible for this work, we present results from two online surveys, which both implement some elements from the Delphi method.

Questionnaire design. In Table 2, we have outlined the build-up of both surveys. The expert and end-user survey contained both open and closed questions, as well as typical Delphi elements, namely the assessment and rating of different factors and their importance, impact, likelihood and desirability of the given scenarios [24]. These were rated on a seven point Likert scale. For sections 3, 4, 5, and 6 in Table 2, and as a result of extensive pre-testing, there were some adjustments in the formulations and ordering between experts and end-users to make them easy to understand for those with less technical knowledge.

Table 2: Questionnaire survey design with Delphi elements.

Section	Examples
1. Introduction	Brief introduction and purpose
2. Screening	Demographics, familiary with IoT
3. Human autonomy	Interpretation of human autonomy in an everyday-life context, and in an IoT context
4. Importance of factors	Assessing the importance of different factors
5. Future optimistic scenario	Ranking the impact of factors that contribute positively
6. Future pessimistic scenario	Ranking the impact of factors that contribute negatively
7. Open-ended questions	Asking for expert and end-users opinions on the potential development of human autonomy in IoT and any additional factors that could be relevant
8. Concluding remarks	Concluding remarks and thank you message

Sample Selection: A list of experts was compiled based on academic literature, policy reports, white papers, and industry briefs, covering IoT, human autonomy, and ethics. The potential respondents were contacted via e-mail and invited to participate in the anonymous quantitative survey. Eventually, 12 experts (among which one woman) completed the questionnaire. These experts all had a comprehensive understanding of current and emerging trends in IoT, as well as the potential implications for human autonomy. To recruit participants for the end-user study, a convenience sampling approach was adopted and the invitation text motivated people who have experience with using IoT technologies in daily life to participate. The recruitment efforts was done through LinkedIn, and several University digital notification boards. In total, 123 respondents completed the survey. Of them, 68.3% identify as women and the biggest age group is 25-34 (43.1%).

4 RESULTS

4.1 Increased focus on targeting autonomy, empowerment, and control in IoT

We first turn to the findings from the SLR and more concretely, aim to map potential existing and future developments / factors that influence human autonomy and how the attention to human-centered design outcomes such as empowerment and autonomy has evolved. As can be observed in Figure 2, user empowerment, and related outcomes such as autonomy and control, are becoming a more critical aspect when designing Internet of Things solutions, as we observe a distinct increase in focus on the topic since 2016.

As shown in Table 3, 62.5% of the literature explicitly states which theory underpins the design principles. 47.5% of the actionable technical design frameworks focuses on designing for the human or the ecological/societal system ("humanistic"), while a nearly equal proportion (45.0%) focuses on the technical abilities of the sensing system, referred to as "rationalistic", and 7.5% on the legal capabilities, referred to as "judiciary".

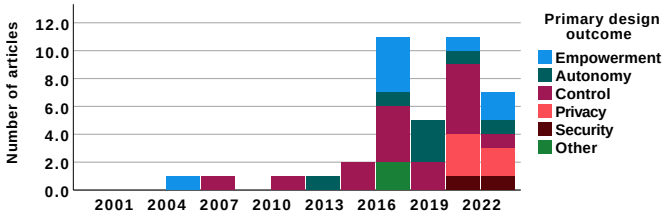

Figure 2: Overview of included articles by year and design outcome.

4.2 Current technical translations

To better understand who is involved in defining human-centered outcomes and translating these technically, we analysed the article set in terms of the background of the author teams. We found that 37.5% of the papers are authored by a single expertise team, versus 62.5% stemming from diverse expertise teams. In addition, 1 out of 2 papers stems from authors from with a Technology background, while 17.5% and 32.5% of the papers come from respectively the Humanities and Social Sciences. Interestingly, a statistical analysis using the Pearson Chi-square test, showed that contributions from technological fields in the analyzed article set are more likely to stem from a single expertise team ($\chi^2(1)= 12.907$, $p < .001$) and

Table 3: Human-centered theory and frameworks.

Design approach	Category (percent)
Theory	Explicitly stated (62.5 %), Not explicitly stated (37.5 %)
Framework	Humanistic (47.5 %), Rational (45.0 %), Judiciary (7.5 %)
Perspective Expertise	Single (37.5 %), Diverse (62.5 %), Technology (50 %), Humanities (17.5 %), Social Science (32.5 %)
Design outcome	Control (40.0 %), Empowerment (20.0 %), Autonomy (17.5 %), Privacy (12.5 %), Security (5.0 %), Other (5.0 %)

more likely to not explicitly state which theory or theoretical fundamentals the work is built upon ($\chi^2(1)= 12.907$, $p < .001$).

Next, we aimed to map how the design outcomes targeting autonomy, empowerment, and control, concretely materialise into actionable frameworks. The findings indicate that humanistic frameworks are nearly always linked to a theory, and all articles that target autonomy use a humanistic framework. Rationalistic frameworks refer less to an underlying theoretical foundation, to explain design assumptions. As can be observed in Figure 3, both humanistic and technical frameworks prioritise control and empowerment as design outcomes. Humanistic frameworks prioritise autonomy as second. Judiciary frameworks are exclusively targeting control and privacy.

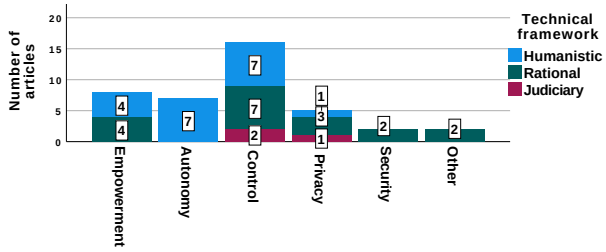

Figure 3: Technical framework and design outcome.

4.3 Interpretations of human autonomy

In the data from the literature, as well as from the survey responses from experts and users, we explored the definition of autonomy in everyday life, as well as how it manifests technically in IoT. In all cases, autonomy can be categorised as either as personal, moral, political, or other [11], as defined in Table 4. As illustrated in Figure 4, most experts interpret autonomy within the realm of personal control, while end-users more often interpret autonomy as having protection from outside influence. Moral autonomy, where the focus is on acting according to your own principles/values, is equally considered in both groups.

In the technical manifestation of autonomy in IoT, there were gaps in the understanding of which outcomes and technical frameworks could promote or undermine user autonomy, also referred to as "freedom to" and "freedom over". Noteworthy, was the lack of focus in the technical development trajectories on the loss of

Table 4: Definitions of human autonomy, [11].

Definition	Question statement
Personal	My ability to be in control of my own life and actions
Moral	Feeling empowered to determine my own path and live according to my own values
Political	The ability to make individual choices freely, not being restricted by others or dictated by technology

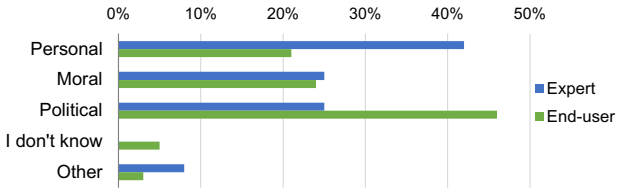

Figure 4: Definition of autonomy: expert vs. user perspective.

human autonomy, by mostly requiring human users to learn or act to preserve autonomy in the IoT sensing system, and in general little assistance in preserving freedom from external influence.

As stated by expert 1: *"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. E.g., 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), safety (e.g., intimate partner violence), and limitations on computing. These are all examples "of freedom from."*

Further, expert 2 pointed out that agency is lost if the human user is required to do something: *"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. Some of the technical solutions might be better qualified as optional, like optional personal privacy recommendations."*

4.4 Scenario/future development paths

In order to understand future development paths that addresses what technically needs to be done in order to protect human autonomy in IoT, we analysed the paths based on the most and least desirable future scenario, then identified topic statements to assess the technical developments' contribution towards either promoting or undermining human user autonomy. These technical manifestations translate into the topic statements and can either promote or undermine human autonomy. The average impact score is calculated from a Likert scale 1-7, where experts and users assess the developments likely impact towards realizing Scenario 1 or 2.

By performing an assessment of two contrasting scenarios we were able to assess the technical requirements solicitation and their impact towards the most desirable solution vs. technical developments and their impact towards the least desirable solutions. Lastly, we aimed to find priority and consensus between experts and users.

The most desirable scenario was outlined as: "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" (**Scenario**

Table 5: Enabler statements presented to the participants in the expert survey, compared with the equivalent in the user survey, deviation $\delta_i = (E_i - U_i)$, average absolute deviation: $\hat{\delta} = \sum_{i=1}^{n} |\delta_i|/n = \sum_{i=1}^{11} |\delta_i|/11 =$ 0.6.

i	Development path	E_i	U_i	δ_i
1	System sends nudges or notifications that warn users of risk-averse situations, i.e., when they are about to share personal data.	4.6	5.8	-1.2
2	Allowing users to customize machine-to-machine automation between IoT devices, i.e., by the use of End User Development methods.	5.1	6.0	-0.9
3	Improved information security and communication network security.	5.5	6.3	-0.8
4	Regulations and legal directives such as GDPR.	5.4	6.2	-0.8
5	Clear conveyance of accountability in complex IoT systems and systems-of-systems.	5.3	6.0	-0.7
6	Personalized privacy recommendations for data sharing and processing in IoT.	4.9	5.6	-0.7
7	Transparency and explainability of IoT systems, allowing users to understand how their data is collected, processed, and used.	5.9	6.3	-0.4
8	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.	6.1	6.3	-0.2
9	The use of frameworks such as privacy-by-design and value-sensitive design when developing IoT systems.	5.9	6.1	-0.2
10	Designing privacy policies that are easy to understand.	5.8	6.0	-0.2
11	Providing innovative interaction strategies for human-to-machine communication, i.e., voice command, user-friendly interfaces.	5.2	5.2	0.0

Table 6: Barrier statements presented to the participants in the expert survey, compared with the equivalent in the user survey, deviation $\delta_i = (E_i - U_i)$, average absolute deviation: $\hat{\delta} = \sum_{i=1}^{n} |\delta_i|/n = \sum_{i=1}^{11} |\delta_i|/11 =$ 0.3.

i	Development path	E_i	U_i	δ_i
1	Third-party interest in gathering information from personal intelligent environments (surveillance).	6.3	6.2	0.1
2	Third-party interest in seeking control over personal environments.	6.3	6.2	0.1
3	Lack or concealment of user configuration capabilities in IoT devices.	5.3	5.5	-0.2
4	Limitations in configurability of IoT, restricting the user's options to predetermined pathways created by programmers	5.5	5.5	0.0
5	ICT developers not recognizing the need for variations in development of IoT devices.	5.0	5.1	-0.1
6	Dependence on centralized authorities and service providers, potentially leading to data monopolies.	5.5	6.1	-0.6
7	The speed of the evolution of IoT is outpacing regulatory processes, potentially impairing effectiveness of regulations.	5.2	6.0	-0.8
8	Limited support for ensuring informed consent in IoT, i.e., giving users the opportunity to accept or oppose data collection and use.	5.5	5.7	-0.2
9	Systemic biases, i.e., in business models, market competition, regulatory frameworks or any other aspects regarding the operational delivery of services.	5.9	5.5	0.4
10	Users do not have complete information about consequences of disclosing data, i.e., systems' collection of position data.	5.2	5.9	-0.7
11	The Digital Divide – unequal access to technology (such as IoT) in society, potentially disadvantaging part of the population.	5.1	5.5	-0.4

1). The least desirable scenario was outlined as: "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" (**Scenario 2**).

In addition to assessing the scenario and the contributing developments, we asked open-ended questions on potential new developments and additional factors that could protect or undermine human autonomy in future IoT solutions. Here, the results indicate a shared agreement between experts and several end-users on the need to consider power and inequalities in the design logic and frameworks, as well as creating novel technical tools/mechanisms that will lead to ease of enacting human autonomy in an IoT context. To illustrate, experts point to the need for questioning who is able to design IoT devices on what premises and with what interests in mind. How are people represented technically, and who is able to act upon the data collected in IoT? Further, end-users in our sample seem increasingly aware of the risk when their private and public life is constantly being monitored, tracked or hacked either by governments, corporations or others.

Personalised privacy settings, control over data, and regulations are deemed important but not sufficient to tackle the challenges, expressed by experts. The end-users maintain that direct and active control of their personal space, mind, and ability to live according to their own individual and societal values is essential. Reaching scenario 1 requires the ability for human users to digitally detox, making *new* choices and possibilities (as opposed to adapt based on existing preferences), and being able to completely opt-out, or shut down the IoT system monitoring, according to end-users' opinion. Agreement is found among end-users and experts for the need to facilitate information clarity, for shared education, and for putting human users in the driver seat of setting up the technical functionalities. Examples are default credentials with all tracking turned off, users control the personalising/learning experience enabled in the technology, understanding user rights to privacy, achieving balance by opting out or digital detoxing, or only violating privacy when the benefit supersedes the cost. Experts unearthed new technical requirements that would ensure that no one can affect anyone else's environment without consent.

5 DISCUSSION

5.1 Prominence and interpretations of human autonomy

There is a marked increase in the literature that address the design outcomes that encompass human autonomy, empowerment, and control (RQ2). A prominent observation from the literature search is the emphasis on multiple outcomes, with variations in interpretation, when designing for human autonomy protection. One important step towards achieving a shared understanding and consensus is to investigate and compare interpretations and variations of design outcomes. The focal point in the literature is designing for human control (40%), followed by empowerment and autonomy with 20% and 17.5%. Each of these concepts entails an element of human control over their choices, life or physical environment. There is a need for dissecting the nuances, on how these concepts are related, underlining the importance of addressing a multitude of closely related design outcomes when building future scenarios that protect or undermine human autonomy in IoT.

Even though, there is a marked increase in literature addressing human autonomy in IoT, it can be argued that there is a majority of "rationalistic"(45%) or "judiciary" (7.5%) technical translations, concerning the future developments paths. As was shown in Table 3, most of the contributions stem from technical teams, and among these, diverse discipline perspectives are over-represented. Both rationalistic and judiciary technical frameworks more often translate human autonomy in terms of maintaining empowerment, control, privacy, security, as opposed to autonomy (see Figure 2). Both experts and end-users stated that these interpretations do not address meaningful autonomy protection technically, as it lacks power for users to counter the loss of control over choices and actions evoked by interacting with intelligent sensing environments.

There is no single agreed upon definition of human autonomy [11], but the conceptual differences in interpretations can be grouped into personal, moral, and political, see Table 4. In order to have future human-centric IoT tools that genuinely protect human agency, the gaps in the interpretations of human autonomy in IoT, indicate a need to design for "freedom from" external influence, as well as "freedom to" act to protect oneself. When comparing the existing literature with the experts and user's definition of autonomy, (see Table 4), the technical solutions are mostly translated from a perspective of personal autonomy. The initial literature search captured technical translations linked to design outcomes with particular focus on empowerment, and control, which mostly indicate a definition of personal autonomy, primarily in single user perspective with the ability to influence decisions and control the sensing environment independently.

Given this observation, it should also be recognized how interpreting autonomy technically as personal autonomy ("the ability of being in control of my own life and actions"), can be a liability for the end-user. More often, end-users interpret the "protection from outside influence" as core to achieving human autonomy in the technical design. In order to design for such protection, or for "freedom from", the technical default should be human control, autonomy protection, *and freedom.* Any definition of freedom when interacting with a technology service requires that a user can have freedom from the loop, from that direct or indirect interaction. However, for users to be able to have the space and ability to be creative, it is also required that humans can evaluate and create a new choice without any external influence/manipulation.

5.2 Future developing enablers and barriers

The alignment and divergence between expert opinions and end-user perspectives on future developing factors, yielded insights into if enablers presented in the literature were actually real enablers with the capability of safeguarding humans' autonomy (RQ1, RQ3). As an illustration, experts and end-users disagreed more on whether the current enablers actually can lead to the most optimistic scenario (Scenario 1), as the end-users consistently rated higher agreement with the statements, as shown in Table 5. The list of enablers presented in the survey, obtained from the literature, was however deemed non-exhaustive by several experts. E.g., education of developers in ethical design of technology, 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.

Conversely, when assessing the impact of future developing barriers, a consensus emerged between experts and end-users on the issues related to surveillance, and third party, commercial corporations vested interest in controlling the intelligent environment and the human users occupying it. These developments had strong impact scores (6.3 and 6.2 respectively, Table 6) and agreement between experts and end-users (δ_i = 0.1) when assessing the contribution towards the least desirable scenario (Scenario 2). This convergence implies a shared recognition of these challenges, signifying the gravity of addressing them to ensure human autonomy protection in the IoT landscape. The studies also revealed gaps that were brought up by experts, such as ignorance among the public, and the lack of technical tools to build genuinely human-centric IoT systems. End-users brought up emerging challenges such as low usability when protecting their human autonomy in IoT. Examples being information overload, detaching users from their experienced reality, ease of being exploited or hacked, and bias/discrimination against weaker groups. Both groups indicate future preferences for greater public control and awareness regarding the technical IoT functionalities, and protection from outside influence, be it governments, corporations, or private, malicious actors.

5.3 Disagreements on personalisation and user-aware technologies

Disagreements centered around the role of personalization and context-awareness in helping human users manage their own autonomy when interacting with IoT services (RQ3). End-users expressed more positive assessments towards personalising functionalities, whereas the experts were more sceptical. To exemplify, experts predicted that the means of providing personalized services may require extensive monitoring and data gathering and processing over time. Moreover, they pointed to that the situated and subjective human experience determines if the service is perceived as beneficial or harmful. As an example, when assessing enabler statement 1 (nudges and notifications about risk-averse situations), we found the highest deviation score (δ_i = -1.2), as shown in Table 5, between experts and end-users, indicating a disagreement in this development having an enabling impact. This could be because it

implies that "the system knows better", as a form of technological paternalism when determining if a risk averse situation exist for human users. As risk and privacy is considered to be a subjective and situated experience, these disparities underscore the complexity of the challenge, and requiring additional knowledge and expertise in order to evaluate and protect against the negative outcomes.

6 CONCLUSION

Through a systematic literature study (n=40) and two Delphi method inspired surveys, this research aimed to shed light on the evolving landscape of challenges and opportunities surrounding safeguarding human autonomy in the context of IoT. While certain divergences between experts and end-users highlight the complexity of the landscape, the agreements underscore critical areas of focus for future scenarios that can safeguard human autonomy in IoT. Distinct agreements warrant attention to lead to the most optimistic future scenario. With this work, we aim to contribute to ongoing pleas for developing informed policies and strategies to protect human autonomy while embracing the benefits of IoT technologies. Follow-up work is needed to identify and analyse the implications for concrete IoT systems and IoT-specific mechanisms to meaningfully safeguard human autonomy.

ACKNOWLEDGMENTS

The authors would like to thank D. Palma and P. Heegaard for valuable help and feedback.

REFERENCES

[1] Madeleine Akrich. 1992. *The de-scription of technical objects.* MIT press, Cambridge.
[2] Janna Anderson and Lee Raine. 2023. *The Future of Human Agency.* Technical Report. Pew Research Center.
[3] Janna Anderson, Lee Rainie, and Alex Luchsinger. 2018. *Artificial intelligence and the future of humans.* Technical Report. Pew Research Center.
[4] Jan Auernhammer. 2020. Human-centered AI: The role of Human-centered Design Research in the development of AI. In *Synergy - DRS International Conference 2020.*
[5] Gianmarco Baldini, Maarten Botterman, Ricardo Neisse, and Mariachiara Tallacchini. 2018. Ethical Design in the Internet of Things. *Sci Eng Ethics* 24 (2018).
[6] Subharthi Banerjee, Michael Hempel, Pejman Ghasemzadeh, Yi Qian, and Hamid Sharif. 2019. A novel approach to social-behavioral d2d trust associations using self-propelled voronoi. *Proc. IEEE 90th Veh. Technol. Conf.* (2019).
[7] Wiebe E Bijker, Thomas P Hughes, Trevor Pinch, et al. 1987. *The social construction of technological systems.* MIT Press, Cambridge.
[8] Mercedes Bunz. 2021. How Not to Be Governed Like That by Our Digital Technologies. Rowman & Littlefield, New York.
[9] Rafael A Calvo and Dorian Peters. 2014. *Positive computing: technology for wellbeing and human potential.* MIT Press, Cambridge.
[10] Bart Cammaerts and Robin Mansell. 2020. Digital platform policy and regulation: Toward a radical democratic turn. *International journal of communication* 14 (2020).
[11] Brandt Dainow. 2017. Threats to Autonomy from Emerging ICTs. *Australasian Journal of Information Systems* 21 (2017).
[12] Sahraoui Dhelim, Huansheng Ning, Mohammed Amine Bouras, and Jianhua Ma. 2018. Cyber-enabled human-centric smart home architecture. In *IEEE SmartWorld.*
[13] European Commission. 2022. Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545.
[14] Expert group on Artifical Intelligence. 2019. Ethics guidelines for trustworthy AI. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68342
[15] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. 2021. A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21).* ACM.
[16] Jose Garcia-Alonso, Javier Berrocal, Carlos Canal, and Juan M Murillo. 2016. Towards Distributed and Context-Aware Human-Centric Cyber-Physical Systems. In *European Conference on Service-Oriented and Cloud Computing.* Springer.
[17] Cristian Hesselman, Paola Grosso, Ralph Holz, Fernando Kuipers, Janet Hui Xue, Mattijs Jonker, Joeri de Ruiter, Anna Sperotto, Roland van Rijswijk-Deij, Giovane CM Moura, et al. 2020. A responsible internet to increase trust in the digital world. *Journal of Network and Systems Management* 28, 4 (2020).
[18] J C Hughes. 2005. Dependence and autonomy in old age: an ethical framework for long term care. *Journal of Medical Ethics* 31, 1 (2005).
[19] Hyunjin Kang, Ki Joon Kim, and Sai Wang. 2022. Can the Internet of Things persuade me? An investigation Into power dynamics in human-Internet of Things Interaction. *Frontiers in Psychology* 13 (2022).
[20] Arto Laitinen and Otto Sahlgren. 2021. AI Systems and Respect for Human Autonomy. *Frontiers in Artificial Intelligence* 4 (2021).
[21] Yair Levy and Timothy J. Ellis. 2006. A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. *Informing Science Journal* 9, 1 (2006).
[22] Harold A Linstone, Murray Turoff, et al. 1975. *The delphi method.* Addison-Wesley Reading, MA.
[23] Maya Malik and Momin M Malik. 2021. Critical technical awakenings. *Journal of Social Computing* 2, 4 (2021).
[24] Ian Miles, Ozcan Saritas, and Alexander Sokolov. 2016. *Foresight for Science, Technology and Innovation.* Springer International Publishing, Switzerland.
[25] María V Moreno-Cano, José Santa, Miguel A Zamora-Izquierdo, and Antonio F Skarmeta. 2015. Future human-centric smart environments. In *Modeling and Processing for Next-Generation Big-Data Technologies.* Springer.
[26] Evgeny Morozov. 2013. *To save everything, click here: The folly of technological solutionism.* Public Affairs.
[27] Claudio Novelli, Mariarosaria Taddeo, and Luciano Floridi. 2023. Accountability in artificial intelligence: what it is and how it works. *AI and Society* (2023).
[28] Carina Prunkl. 2022. Human autonomy in the age of artificial intelligence. *Nature Machine Intelligence* 4, 2 (2022).
[29] Yves Punie. 2017. The Future of Ambient Intelligence in Europe: The Need for More Everyday Life. Routledge.
[30] Yvonne Rogers. 2012. *HCI Theory: Classical, Modern, and Contemporary.* Morgan & Claypool Publishers.
[31] Lambèr Royakkers, Jelte Timmer, Linda Kool, and Rinie Van Est. 2018. Societal and ethical issues of digitization. *Ethics and Information Technology* 20 (2018).
[32] Ben Shneiderman. 2020. Design lessons from AI's two grand goals: Human emulation and useful applications. *IEEE Transactions on Technology and Society* 1, 2 (2020).
[33] Mona Sloane. 2019. Inequality is the name of the game: thoughts on the emerging field of technology, ethics and social justice. In *2019 Weizenbaum Conference.* DEU, Berlin.
[34] Mona Sloane. 2022. To make AI fair, here's what we must learn to do. *Nature* 605, 7908 (2022).
[35] Constantine Stephanidis, Gavriel Salvendy, Margherita Antona, Jessie Y C Chen, Jianming Dong, Vincent G Duffy, Xiaowen Fang, Cali Fidopiastis, Gino Fragomeni, Limin Paul Fu, and others. 2019. Seven HCI grand challenges. *International Journal of Human–Computer Interaction* 35, 14 (2019).
[36] Norbert Streitz. 2019. Beyond 'smart-only' cities: redefining the 'smart-everything' paradigm. *Journal of Ambient Intelligence and Humanized Computing* 10 (2019).
[37] Muhammad Suryanegara, Dimas Agung Prasetyo, Fery Andriyanto, and Nur Hayati. 2019. A 5-step framework for measuring the quality of experience (QoE) of Internet of Things (IoT) services. *IEEE Access* 7 (2019).
[38] Markku Turunen, Daniel Sonntag, Klaus-Peter Engelbrecht, Thomas Olsson, Dirk Schnelle-Walka, and Andrés Lucero. 2015. Interaction and humans in internet of things. In *IFIP Conference on Human-Computer Interaction.* Springer.
[39] Jeffrey Voas, Richard Kuhn, Phillip Laplante, and Sophia Applebaum. 2018. Internet of Things (IoT) trust concerns. *NIST Tech. Rep* 1 (2018).
[40] Ben Wagner. 2019. Liable, but Not in Control? Ensuring Meaningful Human Agency in Automated Decision-Making Systems. *Policy and Internet* 11, 1 (2019).
[41] Jenifer Winter. 2015. Algorithmic discrimination: Big data analytics and the future of the Internet. In *The future internet.* Springer.
[42] Fjørtoft Kaja Ystgaard and Katrien De Moor. 2023. Envisioning the Future: A Multidisciplinary Approach to Human-Centered Intelligent Environments. *Quality and User Experience, forthcoming* (2023).
[43] Kaja Fjørtoft Ystgaard, Luigi Atzori, David Palma, Poul Einar Heegaard, Lene Elisabeth Bertheussen, Magnus Rom Jensen, and Katrien De Moor. 2023. Review of the theory, principles, and design requirements of human-centric Internet of Things (IoT). *Journal of Ambient Intelligence and Humanized Computing* 14, 3 (2023).
[44] Kaja Fjørtoft Ystgaard and Katrien De Moor. 2022. 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.*