Technology in Society 70 (2022) 102026

Contents lists available at ScienceDirect

Technology in Society

journal homepage: www.elsevier.com/locate/techsoc

Trust in the institution and privacy management of Internet of Things devices. A comparative case study of Dutch and Norwegian households

Cristina Paupini [a,*], Alex van der Zeeuw [b], Helene Fiane Teigen [c]

[a] Department of Computer Science, Oslo Metropolitan University, Oslo, Norway
[b] Communication Science, University of Twente, Twente, the Netherlands
[c] Consumption Research Norway, Oslo Metropolitan University, Oslo, Norway

ARTICLE INFO

Keywords:
Internet of things
Privacy protection
Trust
Smart household

ABSTRACT

In a society that is everyday more digitized, the legislation is slowly catching up with the latest frontiers of privacy related vulnerabilities, especially when it comes to the Internet of Things. However, studies have shown that the responsibility for data protection falls more and more on the shoulders of individual users, that are often ill-equipped to recognize threats and take the necessary measures to ensure their right to privacy is respected.

Combining qualitative data from two different interdisciplinary studies, this paper investigates the different cultural traits of the Netherlands and Norway, aiming to answer the research question of how trust in the national institutions influences Norwegians' and Dutch's approach to privacy and IoT devices in the home.

1. Introduction

The home has always been a focal point of society's activities and decision - making, providing shelter and security to its inhabitants [1]. Our society is going through crucial changes in its dynamics, also due to important technological innovations that brought widespread and broadly accessible internet, smaller, cheaper and more powerful sensors, artificial intelligence and machine learning [2]. The Internet of Things (IoT) in particular became the necessary and most distinguishing element of a futuristic imaginary in which objects around us come alive and take care of our daily life performing tasks and services [3]. At the same time, with the ever-increasing demand for connectivity, the risk of data breaches skyrockets [4], as IoT devices often come with a deficiency in proper security systems and upgrade opportunities, especially the ones designed for homes [5].

Security and privacy are part of what Beck (2013) termed the digital freedom risk. Previously, risks were perceived as related to catastrophes such as food safety scandals or atom reactor accidents. However, with the digital freedom risk, there is no destruction or disaster. This new type of risk is the result of successful modernization, created by advances in science and technology, and it interferes with our capacity to control information, which is something we have previously taken for granted. Beck further contends that freedom is always secondary to security. Moreover, it is still to a large degree up to the individuals to seek awareness and information on how to protect themselves, while actors such as the EU are working on regulating and managing privacy [6]. Consequently, the assessment of risk and how risk is being managed falls between individuals and regulating actors such as the EU and national institutions. Moreover, since manufacturers and government policy are often intertwined [7], how individuals perceive risk and how responsible for it they are is determined by cultural aspects.

With the responsibility of managing privacy still in large part on the individual, this paper addresses the existing gap in research regarding how trust in national institutions can influence the user's attitude towards privacy when it comes to IoT devices in the home. To fill this gap, we adopt a unique qualitative approach of cultural comparison research between the Netherlands and Norway to make explicit differences in how government regulations and policies influence how people approach risk and trust with IoT devices in their homes. The Netherlands and Norway both have similarities in internet adoption: high internet penetration, political will to integrate digital technological solutions to societal problems, will and interest among the citizens to use digital tools [8]. However, Amongst European countries and their trust in their national assembly, Norway displays significantly more trust than Netherlands [9]. Meaning that differences that arise between Dutch and Norwegian participants are more likely to be defined by cultural difference in trusting policy. We aim to explore this assumption by answering the following research question:

* Corresponding author.
E-mail addresses: cristpa@oslomet.com (C. Paupini), a.vanderzeeuw@utwente.nl (A. van der Zeeuw), helte@oslomet.no (H. Fiane Teigen).

https://doi.org/10.1016/j.techsoc.2022.102026
Received 8 January 2022; Received in revised form 31 March 2022; Accepted 10 June 2022
Available online 18 June 2022

How does trust in the government and its policies influence Norwegians' and Dutch's approach to privacy and IoT devices in the home?

In our contribution we use a cultural comparison approach from the perspectives of individual users of IoT products. The Data used in this paper comes from the collaboration of two different research projects, from the Netherlands and Norway. Both projects performed semi-structured interviews with participants from different households, multiple home visits and investigated the everyday use of domestic IoT devices and the informant's approach to privacy, with particular focus on privacy in relation to the state and regulating institutions.

The data was merged according to abductive analysis methods [10] and the cultural comparative framework by Thévenot and Lamont [11]. The next section of this paper will illustrate the state of the art and theoretical framework of reference for the research, followed by the methods section illustrating in detail the methodology from both the Dutch and Norwegian studies. In the results section we will start with the similarities of trust between Dutch and Norwegian participants living in the same household to argue that living with the IoT is not very different between the two countries. Differences then arise when comparing how Dutch and Norwegian participants trust manufacturers, their government and policies. We finish with concluding remarks and recommendations for future research.

2. State of the art

2.1. Internet of Things

The fourth industrial revolution is bringing a drastic change of paradigm in our society by introducing widespread and broadly accessible internet, smaller, cheaper and more powerful sensors, artificial intelligence and machine learning [2]. Technology is being more and more intertwined with the very fabric of our society [12], and the more humans become connected, the more they tend to inhabit connected homes. Even the environment itself is becoming widely connected, including in our everyday experience smart cities and vehicles and affecting industries and the public sector as well as individuals [13]. Today, the rapid growth of technology has seen the number of smart devices surge to a staggering 50 billion connected devices [14]. Due to the importance of the Internet of Things (IoT) element in our society, especially in recent years, scholars' interest has been drawn to explore its characteristics in an abundant number of research works, from the pure definitions of IoT and the early stages of its application [15–17] to the effects of its implementation and whether or not Europe is (was) ready for it [2]. Furthermore, several studies explore IoT possible adaptation in smart cities and environments, households and services [18,19]. In the modern depiction of human life, IoT is the key to creating sustainable and connected communities thanks to the power of sensors and the engagement of citizens equipped with smartphones, cloud computing, high-speed networks, and data analytics [20]. For the purpose of this research, IoT is defined as the interconnection via the Internet of computing devices implanted in everyday objects and allowing their management, data mining and the access to the data generated [21].

2.2. The risks connected to Internet of Things

With the ever-increasing demand for connectivity, the risk of data breaches also skyrockets [22]. The Internet of Things has become the setting stone of the futuristic imaginary of a day-to-day reality where objects come alive and actively upgrade our routine [3], but at the same time IoT devices, especially home-based ones, often come with a deficiency in proper security systems and upgrade opportunities [5]. A study from American multinational information technology company Hewlett-Packard (HP) about the most popular devices in some of the most common IoT niches in 2014 reported on an average of 25 vulnerabilities per device: according to the study, "80% of devices failed to require passwords of sufficient complexity and length, 70% did not encrypt local and remote traffic communications, and 60% contained vulnerable user interfaces and/or vulnerable firmware" [23]. Considering that every person in the world is expected to possess, on average, about 25 IoT devices, it is self-evident the impact that such abundance of vulnerabilities can have on our everyday life [24]. The hyper connectivity and interdependence of the smart household devices has an unintended consequence: any device that is connected to the home gateway can serve as a gateway to the entire system. In fact, there have been several well-known security breaches of IoT-devices in later years [4], that only serve to highlight this problem. In his dissertation, Angrishi (2017) argues that these smart devices should be considered as computers that "do specialized jobs", rather than as specialized devices with built-in intelligence [3]. Just like computers, these devices are often run by powerful microprocessors and well inserted in their network through the Internet. What really differentiates IoT devices from computers is that their design often does not include security at all [3]. Some of the reasons for this exposure may be found in their lack of well-defined perimeters, their highly dynamic and mobile nature and heterogeneity in respect to communication media and protocols [25]. Finally, a large percentage of IoT users have little or no awareness of the actual risks involved in connecting devices to the internet, resulting in careless approaches to the privacy settings [26]. The purpose of this paper is to investigate whether cultural differences influence the users' attitude towards these types of devices and in particular their relation to privacy protection.

2.3. The risk society

With the IoT, risks are not particularly noticeable and there is little concern for sudden catastrophes or violations such as with climate change or terrorism. Ulrich Beck described the concept of risk as expressing an intermediate state where we no longer trust our security and believe in progress, but where the expected destruction or disaster has not happened yet [6]. While previous societies were challenged by threats and dangers caused by nature, such as disease, famine and natural disasters, modern threats are created, directly or indirectly, by humans and humans are also responsible for minimizing these risks [27]. Furthermore, these new forms of risk tend to be invisible, and thus require experts to identify and calculate them, and for scientific and media knowledge systems to represent them culturally [28]. Consequently, everyday people must rely on experts to know what the risks are and how to manage them.

At the same time these risks include an individualization of responsibility, bringing risk into everyday life of people and expecting them to seek out knowledge themselves and as such make decisions based on that knowledge [28,29]. Lupton (2016) adds that risk intersects with digital technology in several ways, highlighting three aspects [30]. Firstly, the technologies are not only perceived as mediators of risks, but also sources of them. Secondly, using digital technologies is presented as exposing the users to risks. And thirdly, some social groups are defined as at risk in terms of the digital divide, focusing on a lack of skills, interests or access to digital technologies [30]. This paper touches upon all these streams as it investigates the how and where the users of Internet of Things devices place their trust related to digital risk management. Risk is here narrowed down to security and privacy-related issues with the IoT devices, which is associated with consent, data flow and control. As such, it presupposes that the users share a perception of privacy as a potential risk that needs to be managed.

2.4. Privacy management and trust

With the implementation of the General Data Protection Regulations (GDPR), the privacy management is intended to be placed in the hands of the consumers as a tool of empowerment, to give individuals ownership over their personal data and raise awareness. However,

recent studies show that these aims may not have been achieved. The majority of Norwegians have a passive, non-reflective relation to the GDPR and perceive privacy management as difficult [31]. 70% of respondents to Berg and Dulsrud's study (2018) found privacy settings confusing, while half of them also reported not knowing how they can protect their personal data. In comparison, a Dutch study by Strycharz, Ausloos Helberger (2020) found that the Dutch population shows high awareness of the GDPR and knowledge of their individual rights, but that they doubt the effectiveness of their rights [32].

Moreover, smart home technologies create the challenge of making personal data interpersonal [33]. Certain devices, such as smart lights, robot vacuum cleaners and smart assistants, are often shared within the household and collect data from several persons, although only one set of configurations of the devices is supported at a time. This makes the user empowerment through personal data ownership and control problematic as the households are treated as one unit rather than a set of individuals. Moreover, installing smart home technologies in households creates several non- or "extremely partial"-users within the household, leaving them more passive in relation to the devices even though their data may still be harvested (depending on what type of devices they have) [34]. Pink et al. (2018) write that living with data includes trust. "Living with and having to take responsibility for data manifests itself in the form of mundane and often small but relevant anxieties, which might be experienced as more explicit worries, niggles and sometimes feelings of confusion" (p. 3). To deal with these everyday anxieties, people generate forms of trust that allow them to carry on with everyday life [35].

We explore such forms of trust in this article and in particular the existing gap in research in relation to the influence that trust in national institutions can exert on IoT users. This research offers a unique angle of qualitative cultural comparison that involves the attitude towards IoT and privacy in the domestic context in the Dutch and Norwegian cultural environments.

3. Methods

The projects this research is based on are mostly qualitatively oriented and aimed to gain an understanding of living with smart technologies at home from the perspectives of our participants. Since both projects are set up independently, methodologies differ, including the sample size, and we are careful to note that our findings do not warrant conclusive remarks over either Dutch or Norwegian populations. However, as comparative qualitative research is scarce, especially with emerging technologies, we emphasize the explorative aspect of our research and the conceptual understandings that emerge. Digital technologies have increased the data being studied, but generative sites for data generation via the mundane practices of living with smart-technologies are under examined [36]. That is, big data is used increasingly more for research, but what influences the generative sites that create big data is largely unknown [36]. Our qualitative approach allows us to fill this gap by exemplifying national differences and clarify issues of trust in government policies when living with smart-technologies and generating big data. Therefore, we use an abductive analysis method [10] to substantiate our qualitative findings with comparative cultural theory.

Both Dutch and Norwegian interviews included a walk-along home tour, inspired by Pink et al. (2020) and Coughlan et al. (2013), where the research participants showed the researchers through digital tools such as tablets or smartphones how their technological devices were placed in their home [37,38]. This allowed the researchers to observe the participants engaging with the material environment, infrastructures, and the atmosphere of the home - including other household members. During the interviews, participants were stimulated to offer re-enactments of their experiences with their devices [39].

The Dutch sample consists of 30 households where the main corresponding participants were interviewed five times. Out of the 30 participants, there were nine women and 21 men; aged between early twenties and 65+. Other household members joined the interview whenever they could. Participants were recruited when they had at least one IoT device in their home, different from work or entertainment purposes, and preferably an IoT wearable. Participants were selected to increase the variety in the sample by having unique IoT setups or due to relations with other participants (neighbors, family, friends) that could give additional insight in the social context of the IoT. Interviews were recorded with a GoPro 7 for audio and video data.

The Norwegian sample consists of thirteen participants in ten different households, meaning that some of them were couples living together but interviewed separately. There were eight men and five women in the ages ranging from 24 to 81 years old. Criteria for the recruitment of the household was the possession of either a smart speaker, such as Google Home or Amazon Alexa, or at least three other domestic IoT devices such as smart lightbulbs, Smart heaters, smart hoovers etc. The participants were interviewed twice for about 1 h, and all but one of these interviews took place on digital platforms such as Zoom and Skype.

To analyze our data we used an iterative process between theory and data as described in an abductive analysis approach [10]. We first started with a stage of data familiarization to find similarities between our data. During this stage we compared different IoT setups, concerns our participants voiced, and general patterns of consumption. We found considerable similarities in the different roles taken by members of the household and their trust in each other. This stage was followed by data defamiliarization where we rotated cases to generate conceptual differences. During this stage we utilized the comparative framework for cross-national cultural differences by Lamont and Thévenot [40]. We used this framework as an analytical toolbox to systematically identify repertoires of evaluation between Norway and the Netherlands when discussing the topic of privacy and risk. This framework is based on principles of evaluation that helped us to focus on how our participants make their claims justifiable.

Most important to our analysis are the principles of the 'market' that highlights performance, individuality, and consumer-manufacturer relations; and the 'civic' principles that emphasizes equality, solidarity, and collective wellbeing. Other principles are that of the 'industrial', based technical competences; the 'domestic' on traditional and personal ties; 'inspiration' that involves creativity and emotional development; and 'renown' dealing with public opinion [11,40]. While our Dutch and Norwegian participants make claims that could be justified by composites of different principles, we focus on the market and civic principles as they result in perspectives that logically exclude each other. That is, the aim is not to identify the principles, but rather how we can use these principles analytically to compare statements from our participants in relation to privacy and risk.

The quotations of participants are used because they are illustrative, concise, and insightful without disclosing too much personal information of the participant. The cases discussed are used to demonstrate exemplary differences and gain insight to substantial differences from the perspective of the participants. We are careful not to draw any conclusive remarks over the populations, however the principles that participants utilize are logically exclusive from their perspective. Therefore, we argue that our findings are conceptually generalizable.

4. Findings

4.1. Trust in the family

To start with a baseline in our cultural comparison we find that on the level of households, Dutch and Norwegian participants show very similar patterns. Generally, in a household with two adults, one person is an IoT enthusiast and the other is more concerned about how well the IoT can be made to fit their home [34]. Consequently, we find that the risks about using the IoT correspond to this pattern; one is more

concerned about risks for the other(s) and the other is trusting of its partner. Erik and Frida' Norwegian household illustrates this pattern between responsibility and trust. Erik, who is the self-proclaimed enthusiast and the one who brings the devices into their household, explains how he has the responsibility for privacy and how he tries to maintain this on behalf of both himself and his wife:

> *I think we both agree that having a camera looking into the living room would be kind of creepy. So, we did not do that. Besides maybe having brief conversations about privacy with Google, like the decision to not have Google in the bedroom, she has left me with a lot of the responsibility regarding privacy. But of course, I try to not expose ourselves too much, mainly on the security part (Norway-N).*

While Erik is mainly interested in IoT devices as a hobby, privacy risks do arise and can be a topic of discussion. Still, the responsibility is mainly the part of Erik. This also means that Frida trusts Erik in making those decisions. Frida, on the other hand, is not interested in the technology beyond that it works. Instead, she is concerned with the aesthetics of the household, as she explains the divisions about IoT:

> *I know that he has done some research. So, I actually trust him in that he recommends the best stuff to buy. So that's what I'm doing. I'm relying on him to make that choice. Yeah. Because when I'm actually on, maybe if I go to the shop to Elkjøp or whatever, I'm like: "Oh, I will buy that and that". And they are pushing me to maybe buy something that's much more expensive. And then I end up buying it because … I don't know. I don't have any … You know …. understanding of it. So yeah, I think it's good that he's doing some of the research. I'm more into, like, in the interior and pictures and which color we have to have put on the walls, you know, stuff like that (N).*

The role division between one person doing the research and the other focusing more on how it is integrated with the household is also common with Dutch participants. Such is the case with Anne and Willem, two teachers who lived in northern Norway before returning to the Netherlands. Both are interested in the IoT but, as Anne explains, Willem is the most enthusiastic about it:

> *Willem finds out first, let's say we need a kitchen appliance, then he goes all out and does research, 'this is much better than that'. He really does come up with those things that make you think: "Oh yes, that's right". And then I'm the one who thinks: "do we really need thought or not". So, with smart devices you [Willem] are the one who really does research. In terms of functions what do we need, what do we want with it, but also what are we going to need (N).*

Similar to Erik, Willem researches the IoT devices before getting them and makes the risk assessment, while Anne is more concerned about the necessities of their home. This follows a typical domestic principle based on gendered traditions [40], where women are more included for caring for the home and men are more engaged with maintenance [41]. A crucial addition is that the one doing the research about the IoT products, usually also decides on the safety of the product. As Willem explains when asked if he felt responsible for the privacy of his family:

> *Yes, for sure. That's really in the research before we buy the product. To know how to shield the product or if it's safe. That is why we have consciously chosen not to have a baby camera in the nursery here in the Netherlands. Because lately there have been a lot of reports of things leaking through, and stuff. No, so privacy is important. Also, with the use of Cloud services, and so on (Netherlands-NL).*

Both Erik and Willem consider privacy issues when researching IoT devices, while their partners trust them in their decisions. That is, trust in the other is generally not an issue for Dutch and Norwegian participants, nor do they consider their partners' decisions a risk. What stands out is when Willem explains his situation 'here in the Netherlands'. When asked what he meant with that, he explains:

> *No one lived around us in Norway. So, it would be immediately noticeable if someone came by with a van and stood there. And they don't get much out of that, but here you live with so many people on a small piece of land … That the chance is much more real that something will happen here than it was in Norway (NL).*

For Willem, risk first appears outside the household by comparing Norway to the Netherlands and the density of their living area. Between family members however, trust and responsibility are not an issue for neither Dutch nor Norwegian participants. Generally, the IoT enthusiast is doing the research and, in effect, deciding the risk of IoT in the household. Other household members tend to be trusting of the decisions made by the enthusiast. While Dutch and Norwegians are similar in this aspect, Willem showed how differences arise when trust and risks are discussed outside of the household and corresponding principles of justification are invoked outside the immediate domestic sphere. More specifically, when considering how well their devices and data are being protected, the human-made threat of risk is managed by manufacturers and policy regulations.

4.2. Risky businesses and manufacturers

When participants shift from managing individual risks to the risks managed by manufacturers, participants generally play down the risk of breaches of IoT security. For instance, most do not see the harm of outsiders taking control over their lamps other than an inconvenience. A more pressing concern, in contrast, are the principles of trust participants place in manufacturers and their responsibility over their personal data. Consequently, this is where risks become increasingly intertwined on different levels, between partners within a household, manufacturers, and the level of policy and governance. This is illustrated by Gabriella, currently a Norwegian ICT student, when asked about trusting different manufacturers:

> *I trust technology companies more than stores or chains like Rema 1000 because Google is a technology firm. I think it is harder to trust any company that gets an app as an add-on. It is not a technology company; it is becoming a technology company. Becoming a technological company also means that you have like this old legacy of all technology that you have to work together with. But GDPR has changed very much how concerned I am. Because now the fines are so big that … yeah, that is kind of taken care of (N).*

The GDPR is one of the European sets of laws adopted by Norway as a result of their inclusion in the European Economic Area. Norwegians [31] and our Norwegian participants are, in general, trusting of this framework. It illustrates the compliance with the logic of a civic principle that rules and regulation protect the collective [40]. Consequently, risks are managed simultaneously by the manufacturers and regulatory institutions of the government. While Dutch participants recognize that the GDPR shifts the responsibility of privacy somewhat, they still consider bigger companies a risk. As explained by Joost:

> *I have a responsibility, but with the GDPR law that is mainly a matter for the manufacturer itself. It's very difficult. The last whole story with that medical data from Google and eavesdropping on smart speakers and Siri and stuff like that. I find that difficult. If you look at big companies like Facebook, Google, Apple. No. I don't trust them at all - I'm more afraid of those big companies that they will use or sell it themselves or I don't know what. And those small businesses probably don't have their safety and security in order. That makes it easier to hack. So, it remains difficult (NL).*

Even though Joost starts with his own responsibility, he expects manufacturers to take responsibility as dictated by law. However, unlike Gabriella, the GDPR framework does not translate into trust. Instead, expectations of manufacturers mishandling data persists even within the framework of GDPR regulations. The Dutch participants' perceptions

are as such aligned with the findings of Bauer et al. (2021), where they did not find evidence supporting that GDPR has positively increased trust [42]. One of the main differences, compared to Norwegian participants, is that Dutch participants are less common to refer to a civic principle. Instead, Dutch participants tend to emphasize individual responsibilities between consumers and manufacturers that correspond to a market principle [40]. As a result, risks are managed by the agreements between the consumer and the manufacturer, whether big or small. Such a similar notion can be found with Hans who has a Ring smart-doorbell system. When asked who is responsible for making sure everything is handled correctly with his data, Hans replies:

> *That is my own responsibility because if it says "the 'Ring' has the right to all images that are made to broadcast it or do something with it", then I am the one who agreed to it and who has been stupid. It kind of comes down to that. On that side it is my own responsibility, but I'm not going to read 60 pages in fine print about a bunch of "blah blah blah". So, I think it's my own responsibility, but maybe I'm too easy on it and my idea is that everyone already knows what they want to know. And as long as you pay for data, you'll already be better off (NL).*

Hans emphasizes his individual responsibility by reading and accepting the agreements between himself as the user and Ring as the manufacturer. He also introduces the monetary value as a safeguard for trust. From a Dutch perspective, Hans demonstrates that individual responsibility can easily lead to a market principle without direct civic intervention. This does not mean that Norwegian participants are blind to a manufacturer's monetary goals. This is illustrated by Ivar when discussing the responsibilities of manufacturers.

> *You see from discussions when companies like Google are challenged that they are always on the defensive. They are not taking responsibility in the first place, so they have to be pushed, pushed, and pushed, which is typical for a company that tries to make money first (N).*

Much like Gabriella, Ivar is not blind to the monetary incentives of manufacturers but instead presses hard for more civic engagement in terms of responsibility and managing the risks of the IoT. The GDPR framework can increase trust in manufacturers although most participants may not trust the companies themselves. Instead, our Norwegian and Dutch participants expect that the interests of manufacturers are guided by financial incentives. Consequently, differences arise in the principles by which Dutch and Norwegian participants justify coping with IoT manufacturers. Dutch participants tend to follow a pattern of individualized risk and responsibility rooted in market principles. Norwegian participants, in contrast, tend to push responsibilities for manufacturers rooted in a civic principle and consider risks from using the IoT a problem that is best solved collectively.

4.3. Safety-net of policy

Individual responsibility and the responsibility of manufacturers for managing the risks involved with individual data is intertwined with policy and political intervention. A recurring example of this is the GDPR set up by the EU but also adopted by Norway. While participants trust each other in managing IoT devices, trust in IoT manufacturers is mostly substantiated by trust in policies that hold manufacturers accountable. Consequently, how well participants trust their state and their power to intervene becomes an important factor to assess IoT risk management. This is illustrated by Martin's, who uses Sonos speakers and smart lights by Ikea, reflections on trust:

> *I would be a bit more trusting towards Norwegian companies and Norwegian entities, probably and we know that European companies have the GDPR regulations, which I think gives a bit more security; That they're actually confined in some kind of framework, in a way (N).*

According to Anders, Norwegian companies might be considered more trustworthy, followed by other EU companies due to its GDPR framework. Considerable authority is given to the framework of policy regulations to provide security and confine risks. On a similar note, Ivar calls for more responsibility on part the Norwegian state as large international firms are hard to trust:

> *I think the national state should take much bigger responsibility for developing systems for controlling or surveying and monitoring what is going on. Because it is clear to me that the big international or American firms are not capable of taking any responsibility for all the bad things that could happen with systems (N).*

That Ivar calls for more responsibility by the state can be considered a response that is rooted in a civic principle and contrasts the international or American based manufacturers that operate mainly by market principles. According to Ivar, operating by market principles limits capabilities of taking responsibility and managing risks. Consequently, the call for state intervention for collective problems generally falls in line with a civic principle.

This civic approach is in stark contrast with Klaas, a Dutch participant. For Klaas the interventions by the Dutch the government are considered overbearing. This is explained by Klaas, who has his own company, when asked if the government should take responsibility for regulations about digital data:

> *I do think it is good that certain guidelines are set by the government with regard to privacy. But personally, I think that a lot of things just go too far. Actually, that whole privacy policy … My partner also works in education … Well, I've seen how that has already caused all that trouble in business -what it can do in schools- and then I think: "Guys, it does not make any sense anymore". In that respect, I think everything in the Netherlands has simply gone too far in terms of regulations (NL).*

The aversion to regulation as being restrictive, according to Klaas, is a perspective that tends to limit state responsibility. While both countries use the GDPR, Dutch participants are calling for less intervention, whereas Norwegian participants are calling for more. An explanation for this can be found with Bram. A Dutch participant, when asked about the political system for privacy regulation, much like Hans using a monetary value to safety on an individual level, expects politicians to be similarly motivated by financial gain. As Bram explains:

> *On the one hand it is a good system in itself, but it inherently has that finances are the guiding principles. And the ethical principles play no role in that. I think our society is organized that way. The best thing would be that people would be intrinsically motivated, also business managers and people who are shareholders, but that is not the reality (NL).*

Rather than aligning with a civic principle, Bram applies a market principle to the Dutch government where the market and its financial gains are expected to be the guiding principles. When asked if he would have confidence in the regulation that exists now, he replied:

> *No. Well look, the problem is, of course the politicians can want what they want … You constantly see that companies go under or find other ways. And the things they [companies] do, they are always looking for loopholes in the legislation and it always goes further than you think it goes (NL).*

Bram's explanation for the guiding principles of finance that guides the political system is a reason to distrust manufacturers for managing risks. According to Bram, manufacturers must stay afloat and exploit loopholes in legislation to do so. An alternative would be in Hans' case, where paying for a service helps manufacturers. However, this still relies on trust based on a market principle where money is given to the manufacturers to manage IoT risks. In contrast, a Norwegian perspective would rely on trust based on the financial sanctions for IoT manufacturers imposed by civic engagement. Consequently, civic engagement is also aimed to reduce risk by holding manufacturers accountable, which appears to be lacking with the Dutch participants.

5. Discussion

Norway and the Netherlands are similar in internet adoption by their high internet penetration, political will to integrate digital technological solutions to societal problems, and interest among the citizens to use digital tools [8]. To summarize our findings comparatively, we present the main differences from our findings in Table 1. Table 1 shows the differences between Norway and the Netherlands according to the three dimensions we used in our analysis: the family, manufacturers, and policy. For each dimension we describe with trust dependency how our participants are situating their trust. We then describe how risk emerges from these trust dependencies by comparing between countries. Finally, we identify the cultural principles from Lamont and Thévenot's [11] framework of qualitative cultural comparative research in reference to our findings.

In the domestic sphere, previous research on technologies has shown that the role division between technological proficient user and the main user is traditionally gendered [34,41,43]. The dynamics in the households about the management of IoT devices and their privacy settings seems to evolve in similar ways in both countries: there is a clear separation of roles that usually puts men in charge of managing the devices, while women are focusing mostly on the aesthetics of the household. However, Strengers and Nicholls (2018) suggests that men's responsibility for IoTs may represent a shift in gendered housework, bringing an increased involvement of men in housework in the form of IoT management [44]. Additionally, we find that the responsibilities for decision making on settings and privacy also follow this gendered pattern; as shown in Table 1, women are trusting in the risk management of their partners. Therefore, as a baseline for cultural comparison, we find no reason to believe that there are differences in trust and the management of risks between Norwegian and Dutch participants when it comes to everyday uses of the IoT within the household.

In contrast, we find that our Dutch and Norwegian participants differ the most when they discuss how they trust if manufacturers manage IoT risks sufficiently and how this is intertwined with trust in the state -its laws and regulations-that are supposed to manage the risks created by IoT manufactures. As Humans are also responsible for minimizing risks in their contemporary society [27], IoT devices are perceived as both mediators and sources of risks. Risks exposed by the IoT are not easily managed by individuals alone as they often lack the required professionalism. Consequently, IoT users rely on other parties -IoT manufacturers or the government-to manage IoT risks. Differences in how Norwegians and Dutch participants justify placing their trust in other parties have been illustrated by us using Civic principles and Market principles [40].

Following a civic principle shown in Table 1, Norwegian participants are more trusting of Norwegian and European companies because of the influence their state has and the adherence to the regulations implemented. This is also evident in other studies, showing that Norwegians primarily trusted national online platforms with managing their privacy [31]. They also wish for a stronger presence of the state to manage IoT risks and privacy. However, compared to the Dutch participants, it could be argued that Norwegian participants are too trusting of the government and too reliant on collective action to manage IoT risks. By relying on experts and professionals who come from the civic domain, mostly politicians, minimizing risk can become less of an individual responsibility and might raise concerns for the possibilities of individual interventions. Additionally, an additional layer of policy can have the effect of hiding some of the risks related to the IoT. Paired with upcoming concerns about increased algorithmic decision-making based on big data such as the IoT [45], it can become more difficult for individuals to actively situate their trust. Countries with citizens that generally have similar viewpoints expressed by our Norwegian participants might experience an increased reliance on experts and decreased individual autonomy. Therefore, advice to policy would suggest emphasizing individual responsibilities in managing IoT risks. Professionalizing citizens via digital skills concerning risks and safety is a viable option [46].

The Dutch, on the other hand, appear skeptical towards the intrusion of their state on matters of privacy and support a decentralization of policy concerning IoT risk management, as shown in Table 1. When it comes to the responsibility of manufacturers of IoT devices in the protection of privacy, Dutch participants seem to be more individualistic and drawn to a market principle than Norwegians. Responsibility is placed on the individual and their choices much more than on the companies that have communicated their policy, even if this means going over 60 pages of fine print. This means that risks are related more directly to their digital technologies rather than an additional layer of policy. However, the professionals in which Dutch participants place their trust and manage their risks are often simultaneously the manufacturers. Consequently, The Dutch approach to IoT risks can be considered individualistic while some problems have a higher need for collective action and civic engagement, especially when mega-corporations are involved. It raises concerns about pay-to-play politics and safeguarding individual rights, when individuals feel like they cannot trust their government on digital issues. With the increased use of big data generated by the IoT by manufacturers, better transparency about regulations such as the GDPR and its practical applications will require more attention even if citizens do not call for it themselves.

Table 1
Qualitative cultural comparison between Norway and the Netherlands.

	Norway	Netherlands
Family		
Trust dependency	Partner trusting IoT enthusiast	Partner trusting IoT enthusiast
Risk	Extent of research by IoT enthusiast	Extent of research by IoT enthusiast
Cultural principles	Domestic	Domestic
Evaluation	Esteem	Esteem
Qualification	Trustworthiness	Trustworthiness
Qualified objects	Patrimony	Patrimony
Manufacturers		
Trust dependency	On collective push to manage IoT risk, On national and technological legacy of manufacturers, On manufacturers adherence to GDPR regulations	On Individual proficiencies and responsibilities, On monetary contracts
Risk	Limits of collective engagement, reliance on IoT experts to protect a collective	User agreements, limits of individual expertise
Cultural principles	Civic	Market
Evaluation	Collective welfare	Price and cost
Qualification	Equality and solidarity	Market competitiveness
Qualified objects	Rules and regulations	Freely circulating goods and services
Policy		
Trust dependency	On national state for developing systems for controlling and monitoring, On European regulatory frameworks	On Politicians, On government
Risk	Overbearing regulations, Loopholes in legislation	Financial motivations, Limited individual intervention
Cultural principles	Civic	Market
Evaluation	Collective welfare	Price and cost
Qualification	Equality and solidarity	Market competitiveness
Qualified objects	Rules and regulations	Freely circulating goods and services

6. Conclusions and future work

Although we are aware that our findings do not warrant conclusive remarks over populations, they do offer insightful perspectives on cultural differences that can be applied in future research and policy design. Norway and the Netherlands are similar in the way they approached internet adoption, focusing on high internet penetration, political will to integrate digital solutions to societal problems and high level of interest in using digital tools among the citizens. The dynamics in the households about the management of IoT devices and their privacy settings also seem to evolve in similar ways in both countries: there is a clear separation of roles that usually puts the male in charge of the devices and the decision making on settings and privacy, while the female delegates, focusing mostly on the aesthetics of the household. When it comes to the responsibility of manufacturers of IoT devices in the protection of privacy, Dutch people seem to be more individualistic than Norwegians. Responsibility is placed on the individual and their choices much more than on the companies that have communicated their policy, even if with 60 pages of fine print. Trust in the companies is intertwined with trust in the state and its laws and regulations, and that is where Dutch and Norwegians differ the most: Norwegian people trust more Norwegian and European companies because of the influence their state has on them and the adherence to the regulations implemented. They also wish for a stronger presence of the state in the regulation of privacy and in the development of systems for surveillance. The Dutch, on the other hand, appear skeptical towards the intrusion of their state on matters of privacy and support a decentralization of policy control on the matter.

Future research on this topic could include an evaluation of the impact of the covid-19 pandemic on the users' habits regarding domestic IoT devices and privacy settings as well as a follow up study on the evolution of trust in the institutions in both countries in the aftermath of this global emergency. Additionally, we found the gender differences concerning the management of privacy risk in the household somewhat surprising, especially when involving young couples. A more in-depth exploration on this topic with a focus on how to help the users bridge such gap would surely be of interest.

Acknowledgements

This paper is based on research performed within the "RELINK - Relinking the 'weak link'. Building resilient digital households through interdisciplinary and multilevel exploration and intervention" project, funded by the Research Council of Norway, IKTPluss, grant no. 288663, and headed by Consumption Research Norway (SIFO) and Oslo Metropolitan University (OsloMet) and the research program "Any Thing for Anyone? An individual and Socio-contextual approach to the Internet-of-Things skill inequalities" with project number 452-17-001, which is (partly) financed by the Netherlands Organization for Scientific Research (NWO).

The founding sources had no role in study design; in the collection, analysis and interpretation of data; in the writing of the report; or in the decision to submit the article for publication.

Declaration of competing interest

The authors report there are no competing interests to declare.

References

[1] J. Helle-Valle, D. Slettemeås, ICTs, domestication and language-games: a Wittgensteinian approach to media uses, New Media Soc. 10 (1) (2008) 45–66.
[2] E. Kuruczleki, et al., The readiness of the European union to embrace the fourth industrial revolution, Management 11 (4) (2016), 18544223.
[3] K. Angrishi, Turning Internet of Things (Iot) into Internet of Vulnerabilities (Iov): Iot Botnets, 2017 arXiv preprint arXiv:1702.03681.
[4] B. Budington, Ring Doorbell App Packed with Third-Party Trackers, vol. 27, Electronic Frontier Foundation, 2020.
[5] W. Xi, L. Ling, Research on IoT privacy security risks, in: 2016 International Conference on Industrial Informatics-Computing Technology, Intelligent Technology, Industrial Information Integration (ICIICII), IEEE, 2016.
[6] U. Beck, The Digital Freedom Risk: Too Fragile an Acknowledgment, Open Democracy, 2013.
[7] L.M. Salamon, J.J. Siegfried, Economic power and political influence: the impact of industry structure on public policy, Am. Polit. Sci. Rev. 71 (3) (1977) 1026–1043.
[8] A.J. van Deursen, et al., Digital inequalities in the Internet of Things: differences in attitudes, material access, skills, and usage, Inf. Commun. Soc. 24 (2) (2021) 258–276.
[9] Ø. Kleven, Nordmenn på tillitstoppen i Europa, SSB: Samfunnsspeilet 2 (13–18) (2016).
[10] I. Tavory, S. Timmermans, Abductive Analysis: Theorizing Qualitative Research, University of Chicago Press, 2014.
[11] L. Boltanski, L. Thévenot, On Justification: Economies of Worth, vol. 27, Princeton University Press, 2006.
[12] K. Schwab, The Fourth Industrial Revolution, Currency, 2017.
[13] A. Vulkanovski, Home, Tweet Home": Implications Of the Connected Home, Human And Habitat On Australian Consumers, Australian Communications Consumer Action Network, Sydney, 2016.
[14] T. Alam, A reliable communication framework and its use in internet of things (IoT), CSEIT1835111| Received 10 (2018) 450–456.
[15] L. Atzori, A. Iera, G. Morabito, The internet of things: a survey, Comput. Network. 54 (15) (2010) 2787–2805.
[16] D. Miorandi, et al., Internet of things: vision, applications and research challenges, Ad Hoc Netw. 10 (7) (2012) 1497–1516.
[17] L. Tan, N. Wang, Future internet: the internet of things, in: 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), IEEE, 2010.
[18] E. Bertino, Data Security and Privacy in the IoT, EDBT, 2016.
[19] A. Zanella, et al., Internet of things for smart cities, IEEE Internet Things J. 1 (1) (2014) 22–32.
[20] Y. Sun, et al., Internet of things and big data analytics for smart and connected communities, IEEE Access 4 (2016) 766–773.
[21] B. Dorsemaine, et al., Internet of things: a definition & taxonomy, in: 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, IEEE, 2015.
[22] B.-K. Cheryl, B.-K. Ng, C.-Y. Wong, Governing the progress of internet-of-things: ambivalence in the quest of technology exploitation and user rights protection, Technol. Soc. 64 (2021), 101463.
[23] K. Rawlinson, Hp Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack, 2014, p. 29. HP, July.
[24] I. Butun, P. Österberg, H. Song, Security of the internet of things: vulnerabilities, attacks, and countermeasures, IEEE Commun. Surv. Tutorials 22 (1) (2019) 616–644.
[25] E. Bertino, Data privacy for IoT systems: concepts, approaches, and research directions, in: 2016 IEEE International Conference on Big Data (Big Data), IEEE, 2016.
[26] S. Barth, et al., Putting the privacy paradox to the test: online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources, Telematics Inf. 41 (2019) 55–69.
[27] D. Lupton, *Sociology and risk*. Beyond the risk society: Critical reflections on risk and human security, 2006, pp. 11–24.
[28] J. Tulloch, *Culture and risk*. Social theories of risk and uncertainty: An introduction, 2008, pp. 138–167.
[29] N. Aggarwal, et al., Risk knowledge and concern as influences of purchase intention for internet of things devices, Technol. Soc. 62 (2020), 101311.
[30] D. Lupton, Digital risk society, in: Routledge Handbook of Risk Studies, Routledge, 2016, pp. 319–327.
[31] L. Berg, A. Dulsrud, Tillit og sårbarhet på nett. Forbrukernes praksiser og vurderinger etter innføringen av den nye personvernforordningen (GDPR) i Norge 2018, 2018.
[32] J. Strycharz, J. Ausloos, N. Helberger, Data protection or data frustration? Individual perceptions and attitudes towards the GDPR, Eur. Data Prot. L. Rev. 6 (2020) 407.
[33] M. Goulden, et al., Living with interpersonal data: observability and accountability in the age of pervasive ICT, New Media Soc. 20 (4) (2018) 1580–1599.
[34] T. Hargreaves, C. Wilson, R. Hauxwell-Baldwin, Learning to live in a smart home, Build. Res. Inf. 46 (1) (2018) 127–139.
[35] S. Pink, D. Lanzeni, H. Horst, Data anxieties: finding trust in everyday digital mess, Big Data Soc. 5 (1) (2018), 2053951718756685.
[36] S. Pink, et al., Mundane data: the routines, contingencies and accomplishments of digital living, Big Data Soc. 4 (1) (2017), 2053951717700924.
[37] T. Coughlan, et al., Current issues and future directions in methods for studying technology in the home, PsychNol. J. 11 (2) (2013) 159–184.
[38] S. Pink, et al., Making homes: Ethnography and design, Routledge, 2020.
[39] S. Pink, K. Leder Mackley, Re-enactment methodologies for everyday life research: art therapy insights for video ethnography, Vis. Stud. 29 (2) (2014) 146–154.
[40] M. Lamont, L. Thevenot, Rethinking Comparative Cultural Sociology: Repertoires Of Evaluation In France And The United States, 2000.
[41] A.R. Hansen, et al., Gender, age, and educational differences in the importance of homely comfort in Denmark, Energy Res. Social Sci. 54 (2019) 157–165.
[42] P.C. Bauer, et al., Did the GDPR increase trust in data collectors?, in: Evidence from Observational and Experimental Data Information, Communication & Society, 2021, pp. 1–21.

[43] D. Pal, X. Zhang, S. Siyal, Prohibitive factors to the acceptance of Internet of Things (IoT) technology in society: a smart-home context using a resistive modelling approach, Technol. Soc. 66 (2021), 101683.
[44] Y. Strengers, L. Nicholls, Aesthetic pleasures and gendered tech-work in the 21st-century smart home, Media Int. Aust. 166 (1) (2018) 70–80.
[45] J. Gruber, et al., Algorithm awareness as an important internet skill: the case of voice assistants, Int. J. Commun. 15 (2021) 1770–1788.
[46] A.J. Van Deursen, J.A. Van Dijk, Digital skills: Unlocking the information society, Springer, 2014.

Cristina Paupini is a graduate from the Roma Tre University of Rome with a MA in Education and a thesis in Inclusive education. Her current research focuses on the risks related to Internet of Things in the context of the household and from a Universal Design's perspective. She is a PhD fellow at the department of Computer Science and the Oslo Metropolitan University, where she teaches ethics within the realm of technology use and design to bachelor students.

Alex van der Zeeuw is an Assistant Professor at the University of Twente at the department of Communication Science. He is currently involved in a project on the socio-contextual dispositions of Internet (of Things) use and outcomes. He addresses the transmission and development of skills for using the Internet of Things in human-machine figurations in the domestic sphere.

Helene Fiane Teigen is a PhD fellow at the Institute for Consumption Research Norway of the Oslo Metropolitan University. She holds two master's degrees in media studies, from the University of Oslo and the University of Glasgow. Among other things, she has taken part in an extensive, transdisciplinary fieldwork in Norwegian consumers' households to investigate consumer food handling.