Is the internet watching your cat? A Qualitative Research on Trust in Smart Home Monitoring Devices

Axel van Buren*
a.w.p.vanburen@students.uu.nl
Utrecht University
Utrecht, Utrecht, Netherlands

Yangfan Chen*
y.chen40@students.uu.nl
Utrecht University
Utrecht, Utrecht, Netherlands

Abstract

Imagine you are scrolling the internet and out of nowhere you find pictures of yourself on the toilet. This concerning incident involved a woman in Brazil, where her privacy was breached through images captured by her smart vacuum. As smart technology evolves, the risk of data breaches intensifies. Utilizing qualitative research methods, this study explores how people view these smart home monitoring devices. A focus group approach is employed to uncover how the factors: of concern, comfort, trust and convenience, shape public opinion. Using these factors, the study engages in a creative problem solving session to devise strategies that could enhance trust and acceptance of smart home monitoring devices. This research aims to offer insights into improving the relationship between consumers and smart technologies, ensuring greater security and trust.

CCS Concepts: • **Human-centered computing → Empirical studies in HCI**.

Keywords: smart cameras, Internet of Things (IoT), privacy, personal data, data breaching, design

ACM Reference Format:
Axel van Buren and Yangfan Chen. 2024. Is the internet watching your cat? A Qualitative Research on Trust in Smart Home Monitoring Devices. In *Proceedings of Utrecht University Human Computer Interaction Qualitative Research Studies Conference (INFOMQLM '24).* ACM, New York, NY, USA, 16 pages. https://doi.org/XXXXXXX.XXXXXXX

1 Introduction

With the development of Internet of Things (IoT) technology, smart home monitoring devices have transcended their traditional role as mere security devices. These devices, defined as smart home devices that integrate cameras, now serve multiple purposes, including enabling remote interaction with pets, facilitating communication with delivery personnel at the doorstop from the kitchen, alerting abnormal situations to the user's smartphone, and capturing moments of daily life for the increasingly popular short video platforms. Yet, this progress is a double-edged sword. While bringing considerable convenience, these devices' enhanced capabilities raise concerns about personal privacy [9] as they require capturing more sensitive and private content and uploading them to cloud services. These concerns are not merely theoretical. For instance, Ring, a smart home camera company, was compromising customer privacy by allowing any employee or contractor access to consumers' private videos [3], and iRobot, a smart vacuum company, breached a considerable amount of private photos, including sensitive images of people in their bathroom [4]. While these concerns are supported by the mentioned and other data breaches, insufficient research has been done to study the security and privacy concerns of people who own or potentially want to have smart home monitoring devices. Some research on user perceptions of smart speakers [1][2][7] and other smart home products have been done, but only a few studies focusing specifically on smart home monitoring devices [5][9].

This research aims to bridge this gap by conducting qualitative research with two aims. Firstly, this research aims to understand people's thoughts about smart home monitoring devices. Secondly, with these insights, this research aims to propose potential solutions to enhance people's trust towards smart home monitoring devices. While improving security technology and implementing comprehensive privacy and security measures are more radical solutions, technology and management perspectives are not in the research scope. This research prioritizes people's perceptions of trust and solutions that can be applied by smart home monitoring devices companies. More specifically, our research questions are as follows:

RQ1: *What are people's experiences, perceptions, and concerns regarding smart home monitoring devices?*

[*] Both authors contributed equally to this research.

INFOMQLM '24, January 25, 2024, Utrecht, Utrecht, Netherlands

ACM ISBN 978-1-4503-XXXX-X/18/06
https://doi.org/XXXXXXX.XXXXXXX

RQ2: *How to enhance people's trust in smart home monitoring devices?*

Two approaches are used to address these research questions. Firstly, focus group sessions were conducted to collect people's experiences, perceptions, and concerns regarding smart home monitoring devices. The result of the focus group method is used to address RQ1. Secondly, with the insights from focus group sessions, creative problem solving sessions were conducted to collect potential solutions. The final solutions to address RQ2 are based on the results of both the focus group method and the creative problem solving method. Further research can facilitate insights gained from this study, and companies that produce smart home monitoring devices might get inspiration from this study of how to enhance their products.

2 Background and Related Works

2.1 Smart Home Monitoring Technology

In this section, we present a summary of current smart home monitoring technology, which is based on our review of popular smart home monitoring devices' product pages and manuals.

Compared to traditional video monitoring technologies, the foundation of smart home monitoring devices is built on cloud-based applications and pattern recognition. This technology, combined with accompanying product designs, enables the following features:

1. **Live video and audio feed.** Most smart home monitoring devices allow users to check video/audio footage remotely. Some of these devices allow two-way voice interaction which enables users to communicate with people (e.g. smart doorbell) or interact with pets (e.g. indoor smart camera).
2. **Smart alerts.** Some devices provide smart alert features based on motion detection, object recognition, voice recognition and sometimes facial recognition. The alerts of certain events will be sent to users directly. However, previous research also points out that the object/pattern recognition features are currently inaccurate and time-consuming [5][8].
3. **Timeline history with events highlights** Most smart home monitoring devices enable online footage storage and offer a timeline history feature with event highlights. With these pattern recognition capabilities, these devices can pinpoint important events, saving users hours of review time in some cases. Currently, the inaccurate recognition issue also appears in this feature. [8].
4. **Activity zone.** This feature enables users to designate a specific area within the camera's field of view so that notifications are triggered by particular types of activities occurring specifically in that zone. [6]

2.2 Related Research in Smart Home Monitoring

2.2.1 The usage of smart home monitoring devices.

Recent empirical work groups the usage of smart home monitoring devices into four categories: [5]

1. **Behavioral deterrents**. Using the devices to deter harmful or illegal behaviours.
2. **Interpersonal Communication**. Communicating with visitors, co-dwellers, or pets.
3. **Documentation Devices**. Documenting footage for memorizing, and sharing. Evidencing what happened.
4. **Device Actuation Systems**. Configuring the devices to send notifications for certain events and automatically capture video/audio.

The prevalent social media and short video platforms also shape the smart home monitoring market. For example, videos about fun, unexpected moments with cars are popular in Tiktok, a leading short video platform. Many of these moments are captured by smart home monitoring devices. This implicates potential changes in marketing strategies, consumer engagement, and the development of smart home technologies that resonate with contemporary digital lifestyles.

3 Study Design

The study attempts to answer the research question proposed in the introduction. By use of the following qualitative research methods, at first focus groups are conducted to gain insights into the perception of people considering smart home monitoring devices. Using these insights the creative problem solving session is held, to handle the issues found in the focus group. Using the combined results from both research methods and thorough analysis the answer to the research question is concluded.

3.1 Focus Group

In this research focus groups (FG) were conducted as a basis for the creative problem solving session. The focus groups aimed to gather informative insights and understand the issues people have with smart home monitoring devices. Based on the results from the FG, the problem statements for the creative problem-solving session were established and the concerns of the participants were recorded.

3.1.1 Method. The main reason for using the focus group as the first method is the fact that **a FG allows for all participants to be able to share their own experiences**. The participants are all able to indicate the issues they encounter with smart home monitoring devices. This equal opportunity of participation allows for a wider range of opinions and gathering useful insights. **Secondly, the usage of a focus group reduces the heuristic thinking of participants** as they are all exposed to each other's opinions, gaining new

Table 1. Participants of FG Sessions

Session	Gender	Occupation or Background
1	Female	HCI Master's student
	Male	HCI Master's student
	Male	HCI Master's student
	Male	HCI Master's student
	Male	HCI Master's student
2	Male	Software engineer
	Male	Software engineer
	Female	UI/UX designer
	Male	UI/UX designer
	Female	BSc Communication and Journalism

insights different from their own. This also allows for participants to engage in active discussion, which is an active preliminary assessment of the discussed information. Leaving the thoroughly discussed opinions as final results for the researchers. **Lastly, this all leads to the information needed to lay the groundwork for the creative problem solving session.**

3.1.2 Participants. Convenience sampling and snowball sampling methods were used to recruit participants for the Focus group sessions. Two focus group sessions were conducted during the research period. One session was conducted with five students in the course "Advanced Qualitative Research Methods for HCI", while the other session was conducted with five participants with differing occupations and backgrounds. These sampling methods, having classmates and friends participate and gather other participants for this research, might have caused some bias related to the IT background. However, these are the more informative and knowledgeable sources for this research topic. The overview of participants can be found in Table 1.

3.1.3 Materials and Preparations. The following materials were gathered and prepared before starting the focus group, an information sheet (see Appendix C), a consent form (see Appendix E), a pen and 2 different coloured post-it notes were prepared for each participant. A circle of seats around a table was formed for all participants. The microphone was placed in the centre of the table. Refreshments were served on the table as well. The participants were then welcomed and asked to join the focus group where instructions and clarifications were then provided. One of the researchers had the prepared protocol and led the focus group, while the other researcher used the laptop to take notes and record the findings.

3.1.4 Procedure. The first focus group was hosted in one of the classrooms at Utrecht University and the second session was held in the house of one of the researchers. In each session, participants were seated around a table to be able to actively engage in discussion with each other. In both sessions the participants had all the given material in front of them on the table and were all seated around the microphone. The protocol of the focus group contains 3 main stages, opening the FG, the discussion and the closing of the FG. The entire detailed protocol can be found in the Appendix A, but a summary is as follows:

Opening the focus group. The participants were welcomed and asked to join the focus group where instructions and clarifications were then provided. The researchers introduced the topic and asked the participants to fill out the consent forms. Having the participants consent to participating and also being recorded for the eventual results. The focus group was then opened according to the script provided in the protocol (see Appendix A). The use of the post-it notes was explained and the focus group was ready to begin.

The discussion: Gathering opinions. The structure of the focus group was to first introduce the topic and get the participants comfortable with the topic at hand. By discussing their own experiences with smart home monitoring devices, the researchers gained insights into the participants' usage and general opinions.

The discussion: Scaling the factors. Proceeding to then have the participants look at both sides of using smart home monitoring devices, and write 1 argument in favour and against on the provided post-it notes, causing the participants to actively weigh the different opinions on smart home monitoring devices. By then using their answers as discussion topics, and having all participants scale the levels of concern, convenience, comfort or trust, the heuristic thinking was reduced and the discussion was broadened. The participants were also asked to provide reasoning besides their scaling.

The discussion: Scenarios. The focus group then proceeded to focus on certain scenarios of prepared use cases concerning smart home monitoring devices. Where all participants were asked if they felt comfortable in those scenarios and why they felt that certain way. This was done to gain more insights on specific known cases and to measure the severity of some issues participants have with smart home monitoring devices to then use for the creative problem session.

The discussion: Break. A break was held, to have the participants relax a bit and make use of the refreshments.

The discussion: Improving trust. The final part of the focus group had the goal of gaining insights into gaining trust. By having the participants discuss how their own opinions on smart home monitoring devices could be positively influenced, and what these influential factors are. This led to a broad discussion on several factors which gave the researchers insights and inspiration for the creative problem solving session.

Closing the focus group. The focus group was then closed according to the protocol, summarising the entire focus group shortly, having participants agree to that summary's correctness and thanking the participants.

3.1.5 Analysis.

The analysis of the FG results is made up of 4 steps. **Firstly, the recorded audio will be transcribed into a text file.** Having the full transcript of the focus group allows for a full analysis of the entire session. **Secondly, the scaling questions** are analysed for their results and turned into gauge diagrams displaying the opinions of the participants. Showcasing the entire spread of opinions and the average, displaying a clear image of the participants' opinions on the several matters discussed. **Thirdly, coding the transcript** is done to recognize the important and frequently mentioned factors discussed by the participants in the focus group. **Finally, the groundwork for the creative problem solving session is established**, based on the transcript, sticky notes and summary that resulted from the focus group. The results provide a clear understanding of the major issues people have with smart home monitoring devices.

3.2 Creative Problem Solving

In this research, Creative Problem Solving (CPS) sessions were conducted to collect ideas to address our research questions.

3.2.1 Method.

There are two reasons for selecting CPS as the second approach. **First, CPS allows a direct exploration of how to address the research question.** The CPS method allows a structured way of brainstorming which enables systematic collection, categorization, and evaluation of possible ideas. Conducting CPS sessions among people outside of the researcher's environment can help us across the egocentric empathy gap and mitigate availability bias. Conducting CPS sessions among groups of participants can help the group build a solid and broad context of the problem and yield a more comprehensive and larger amount of ideas. **Second, the CPS sessions in this research can greatly utilize the findings of focus group sessions.** The findings of focus group sessions can provide insights into people's experiences, perceptions, concerns, and factors that can alleviate their concerns regarding smart home monitoring devices. By referring to the findings of the focus group sessions, the focus of the discussion can be narrowed down, so that the common issue of CPS that the discussion may be broad and vague can be mitigated. The findings of focus group sessions can also contribute to the evaluation of the collected ideas from CPS sessions.

3.2.2 Participants.

The convenience sampling method was used to recruit participants for the CPS sessions. Two CPS sessions were conducted during the research period. One session was conducted with five students in the course "Advanced Qualitative Research Methods for HCI", while the other session was conducted with five participants with various occupations and backgrounds, mostly related to the IT industry. The sampling methods might cause a bias towards young adults with an ICT background. However, it also ensures a high level of problem solving skills regarding the ICT-related research problem of this research. The overview of participants can be found in Table 2.

Table 2. Participants of CPS Sessions

Session	Gender	Occupation or Background
1	Female	HCI Master's student
	Male	HCI Master's student
	Male	HCI Master's student
	Male	HCI Master's student
	Male	HCI Master's student
2	Female	Software engineer
	Male	BSc Computer Science
	Male	Graphic designer
	Male	MBO IT student
	Female	BSc Communication and Journalism

3.2.3 Materials and Preparations.

An information sheet (see Appendix D), a consent form (see Appendix E), a marker and some large-size post-it notes will be prepared for each participant. Depending on the site of the CPS session, a table or a whiteboard was used to place all post-it notes from participants. A microphone was placed in the corner of the table or held by one of the researchers. Refreshments were served nearby.

3.2.4 Procedure.

The first CPS session was organised in one of the classrooms at Utrecht University. In this session, participants were standing circularly around a whiteboard. The second CPS session was held in the house of one of the researchers. In this session, participants were standing around a large table. In both sessions, participants walked around the whiteboard or table freely with a marker and some post-it notes in hand. The protocol of the CPS sessions consists of five stages. The detailed protocol can be found in Appendix B. A brief description of each stage is as follows:

Introduction. In this stage researchers first welcomed participants one by one and distributed information sheets and consent forms. Participants were then gathered around the whiteboard or table. Researchers then introduced the topic of the CPS session, and summarize people's perception and privacy concerns regarding smart home monitoring devices, as well as the factors mentioned in the focus group sessions that people think can alleviate their concerns. After that, the topic of the CPS session was mentioned again. At the end of the introduction, participants were asked to introduce themselves and state if they had heard of any smart home monitoring devices.

Idea generation. In this stage participants were asked to start thinking about ideas that can address the stated question. The ideas were written down in a post-it note using a marker and then stuck to the whiteboard or table. Participants and researchers would re-arrange the post-it notes in the whiteboard or table if some connections were found.

Story excursion. When new ideas stopped coming out and the total amount of ideas was not sufficient, the researchers would organise a story excursion. The excursions were started by a starting line of a story from researchers. Participants were required to come up with a sentence that contains a plot twist of the story. Researchers hosted two rounds of this process for each story excursion. After the excursion, participants were asked to check the current whiteboard or table and continue the idea-generation process.

Participants evaluation. After the idea generation, each participants were told that they had three votes for the ideas. Participants voted their favourite ideas one by one by drawing a mark on the post-it notes.

Ending At the end of each CPS session, the researchers asked the participants if they wanted to add anything or had any questions. After that all participants were thanked again and the session ended.

3.2.5 Analysis. The analysis of the CPS results consists of three steps. **First, the recorded audio will be transcribed into a text file.** The following steps are based on the transcript of the CPS sessions. **Second, ideas are identified and categorized.** In this step, repeated or similar ideas are merged into one idea. **Third, the categorized ideas are preliminarily filtered.** In this step, ideas from perspectives that are out of hardware or software design will be filtered out. For example, ideas from laws and regulations' perspectives are filtered out as it is not in the scope of this research. Meanwhile, ideas that are generally impractical are also filtered out. **Finally, the Strengths, Weaknesses, Opportunities and The strengths (SWOT) analysis method is applied to evaluate the filtered ideas.**

4 Results

4.1 Focus Group

After two focus group sessions were conducted, the recordings were transcribed. By extracting the transcript, initial coding was founded and themes were developed. This section will start from an overview which is the result of four scaling questions designed for the focus group. After that five themes will be discussed. The result of the scaling questions matched the result of the five themes.

Four scaling questions were asked during both sessions. The scaling questions are about the following four factors:

1. **Comfort.** This factor is the aspect of feeling safe using the devices on a daily basis.
2. **Trust.** This factor explains the aspect of feeling safe in the agreement between the company and the customer.
3. **Concern.** This factor explains the aspect of fear of misuse by third parties.
4. **Convenience.** This factor explains the aspect of user-friendliness and laziness.

The results of this quantitative scaling can be seen as an overview of the result of the focus group sessions (See Figure 1). From this figure, we can see that while the level of convenience is high, the level of comfort and trust is low and concerns regarding home monitoring devices are also high.

Five developed themes are discussed in the following sections.

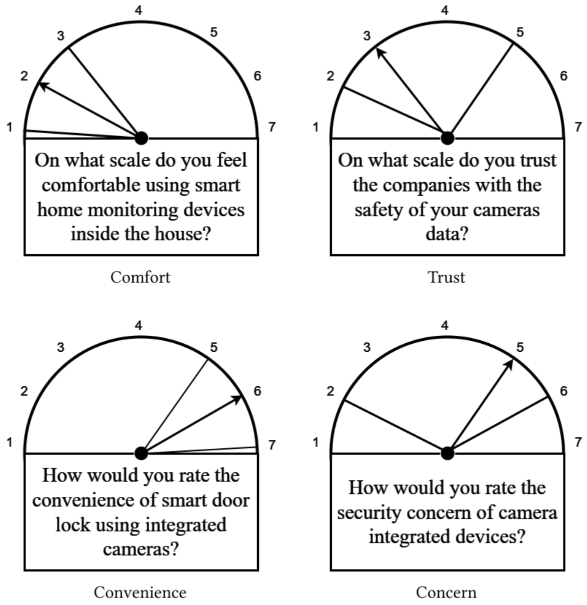

Figure 1. Average comfort, trust, convenience and concern level of participants concerning the stated question.

4.1.1 Convenience and concerns in pet monitoring.

In the two focus group sessions, four out of ten participants have/had pets in their living space and three out of them installed smart indoor/pet cameras in their living space. According to Participant Quotation 1 (PQ1) and Participant Quotation 2 (PQ2), the use of pet cameras brings significant convenience. Meanwhile, there are also concerns (e.g., PQ3). However, the convenience outweighs concerns and trust issues in the use case of pet monitoring.

PQ1: *"I would say it is quite common to use a pet camera if you have cats. For me, I am usually out of my room like 8 or 10 hours a day so I want to check from time to time how my cat is going and that's why."*

PQ2: *"I bought it not very long after I had my cat. I think it is because I was planning a trip during the weekend and I don't want my cat to be a... Schrodinger's cat. I thought I could use a pet camera so that I could ask my friend to rescue my cat if necessary."*

PQ3: *"I put the cameras at the desk of my room and the camera is somehow capturing my wardrobe. And ever since I had it, I have intentionally avoid changing dress there even though I used to be. "*

4.1.2 Trust in different brands.

During the two focus group sessions, perspectives about brands and how to choose brands are frequently mentioned. However, there are two different opinions about it. Firstly, the majority of participants agreed that brands with good reputations, although they are not sure what sources or criteria should be used to measure the reputation of certain brands (See PQ4). One participant mentioned a different point of view (See PQ5) that no brand can be flawless regarding data and privacy security, and therefore they will always keep a low level of trust in all brands. Other participants in that focus group session expressed agreement with this statement.

PQ4: *"I certainly will choose a camera from some brand I trust or say has good records. I mean brands without serious data leak incidents...Oh I am not sure if there is any database about that, so it might be challenging [to evaluate the brand reputation]. I don't know, maybe the government should build one."*

PQ5: *"That's all true but I think as long as you have to upload data to their server, there is always risk of leaking. For me I don't even trust iCloud, I will not trust my pet camera at all so I will always be cautious."*

4.1.3 Concerns about the smart alerts feature.

Smart alerts feature detects abnormal or worthwhile events and notifies the device owner. The accuracy and reliability issue was mentioned in the second focus group section and the other two participants who own a smart home monitoring device strongly agree with it (See PQ6). This feature then drew the participant's attention and one of the participants pointed out that this feature probably relies on cloud computing, so concerns about uploading footage to a cloud server arose in the focus group session (See PQ7).

PQ6: *"About the convenience, I am quite annoyed by the notification ability of my camera, it is just not accurate and sends me a lot of irrelevant or false alarms. "*

PQ7: *"I don't think the camera itself can do this level of pattern recognition, if so, that means your data may be constantly uploaded to the server. And I also guess this kind of technology will use deep learning, so your data might be collected and sent to someone that annotates the image."*

4.1.4 Convenience generally outweighs concerns.

Besides the use case of pet monitoring (see Section 4.1.1), the discussion about weighting convenience and concerns also appears frequently. One participant who used to live in the US mentioned that he will install smart doorbells in the future (See PQ8). In another focus group session, one participant also mentioned that installing a smart doorbell and indoor/pet camera is natural for them because it is "their lifestyle" which means a complete smart home setup including lights, smart speakers, etc. (See PQ9).

PQ8: *"Personally, it depends on where I live, but I definitely consider it... I think there's just a lot of stuff that can happen right outside your door, either thieves or violent individuals that can come to your place. Sometimes you need to have certain kind of evidence to present to the police in order to help you in those cases. And at least knowing people you need to avoid. "*

PQ9: *"Still, I will buy one of those just because it is how I like, my lifestyle. I am very interested in the concept of smart home and I will definitely build mine."*

4.1.5 Non-primary user concerns.

The topic of non-primary user concerns is mentioned in one focus group session. In the participant's relative's house, they install an indoor camera for their naughty dog. This camera is located in their living room. The participant stated that she is always aware that there is a camera in the living room every time she visits even though she has no problem with it (See PQ10). However, this topic is only mentioned once by one participant. Even though it is a worth noticing theme, due to the time frame, no more focus group session was conducted to better understand this theme.

PQ10: *"One of my relatives installed a indoor camera because they have a quite troublesome dog. So every time I visit I am always aware that there is a camera in this room. Although I am OK with it, the thought just keeps appearing and no kidding I felt like I self-reflect way more than usual"*

4.2 Creative Problem Solving

After transcribing audio, cleaning data, identifying, clustering and removing repeated ideas, 12 ideas were collected in the first CPS session and 14 ideas were collected in the second CPS session. The collected ideas from the two sessions also overlap. In the end, 18 unique ideas in total were identified. Six ideas were filtered out and 12 ideas were selected for the continuous SWOT analysis (see Table 3).

These 12 ideas can be grouped into three overlapping categories, which are: (a) software features, (b) public relations, and (c) product design. The full SWOT analysis result can be seen in Table 4.

Table 3. Collected ideas and preliminary filtering result

	No.	Idea
Incl.	1	Provide detailed access logs/records
	2	Use strict login authentication
	3	Publish regular reviews of security system
	4	Give privacy protection commitment
	5	Provide high quality user interface
	6	Ensure high data usage transparency
	7	Delete clips with specific faces
	8	Blur all humans before uploading
	9	Stop recording when users are at home (e.g., via Wifi connection)
	10	Use physical camera status indicator
	11	Physically isolate the camera when turned off (e.g., face backwards, close the lens cap)
	12	Provide data breach history archive
Excl.	13	Apply high encryption standards [Exclusion reason: Security technology is out of the research scope]
	14	Localized data storage. [Exclusion reason: It significantly downgrades functionality of smart home monitoring devices]
	15	Allow deploy on privately hosted servers [Exclusion reason: Impractical. It requires high IT technical skill]
	16	Establish laws about fine and compensation for data breaching incidents [Exclusion reason: Laws and regulation is out of the research scope]
	17	Storage data at third party's server [Exclusion reason: Security technology is out of the research scope.]
	18	Let customers become shareholders [Exclusion reason: Impractical]

Based on the result, four potential solutions are proposed to address the research question. The solutions are formulated from the ideas with modifications and combinations.

4.2.1 Detailed access and operation records.

This solution derives from a frequently mentioned idea from the creative problem solving sessions. The related participants' quotations are as follows:

PQ11: *"It would help if there is a place to store all the records of who access what data. This way it gives people a feeling of control, people will feel safe if there are no unknown people in the logs and the missing of logs might cause users to feel suspicious."*

Similar participant's quotations are omitted here. The difference between them from PQ11 is: (a) Also record how unknown users access the data. (b) If the data is uploaded to the cloud even by the manufacturer, there should be records, too. (c) Notification should be sent to the owner if an unknown user accesses.

Based on this discussion and the SWOT analysis result, we formulate this solution as follows: this solution involves creating an advanced logging system within the software that records every user login, data access and operation. This log would include timestamps, user identification, IP address, and details of the actions taken. For requests that are from previously unknown users, a notification will be sent to every existing user in the list.

The advantages of this solution are: (a) It provides a real-time monitoring of device access which can be used to quickly identify unauthorized usage. (b) It increases the data transparency of the camera footage. (c) It enhances user control and awareness, which will improve user's low level of trust as mentioned in the result of the focus group method.

The potential challenges of this solution are: (a) The design of the presented logs to users is challenging. Detailed logs can be too complicated for most users, which will cause them to just ignore them, therefore reducing effectiveness. (b) The records themselves have risks of being targeted in a data breach, which compounds security issues.

4.2.2 Tangible camera status.

Tangible status in smart home monitoring devices can be manifested as visible indicators such as LED lights, mechanical shutters, and camera orientation. The use of tangible camera status can clearly show when the devices are not recording (e.g., LED light off, mechanical shutters closed, and the camera pointed to the ceiling or backwards).

Even though participants in the creative problem solving sessions did not mention the term "tangible", they proposed a considerable amount of ideas that are related to this concept. Several variations of tangible status indicators are mentioned: (a) physical cap that only is removed while recording; (b) use of different LED light colours to indicate different statues; (c) the face of the camera backwards or downwards while not recording.

The advantages of this solution are: (a) This would directly address privacy concerns by making the camera's status evident to everyone in its vicinity. (b) It would also build user trust, as they can easily tell when they are being recorded. Also, this solution addresses the problem mentioned in section 4.1.5, which is about non-primary user concerns. For non-primary users, a clear indication of recording and not recording can significantly alleviate the problem theme from the focus group result.

The potential challenges of this solution are: (a) It is challenging to design a clear indication for the user to understand. (b) For some visible indicators, there is also the risk of them being manipulated or malfunctioning, which could falsely reassure users about their privacy.

Table 4. Summary of the full SWOT analysis of collected ideas

No.	Idea	Strengths	Weaknesses	Opportunities	Threats
1	Provide detailed access logs/records	Enhance user transparency and security awareness.	Risks overwhelming users with too much information.	Opportunity to differentiate with advanced user control features.	Potential privacy concerns if logs are mishandled.
2	Use strict login authentication	Significantly improve security against unauthorized access.	May inconvenience users with complex login processes.	Opportunity to integrate innovative authentication technologies.	Risk of user lockout due to authentication errors.
3	Publish regular reviews of the security system	Build trust through ongoing commitment to security.	Could expose and highlight security vulnerabilities.	Chance to engage and educate users on security practices.	Competitors may exploit disclosed weaknesses.
4	Give privacy protection commitment	strengthen brand reputation for privacy-conscious consumers.	Legal and operational challenges in maintaining strict privacy.	Sets a precedent for industry privacy standards.	Reputation damage if privacy commitments are breached.
5	Provide high quality user interface	Enhances overall user experience and satisfaction.	Requires continuous investment in design and updates.	Attracts a wider user base with ease of use.	Competition with other advanced interfaces in the market.
6	Ensure high data usage transparency	Increases trust through clear communication on data usage.	Complexity in presenting data usage in an understandable way.	Differentiation in a market often critiqued for opaque data practices.	Potential user confusion or misinterpretation of data practices.
7	Delete clips with specific faces	Offers enhanced privacy through selective data management	Relies on the accuracy and reliability of facial recognition technology.	Unique feature that addresses specific privacy concerns.	Ethical and legal issues surrounding the use of facial recognition.
8	Blur all humans before uploading	Provides a strong privacy measure by anonymizing individuals.	May reduce the practical utility of the footage.	Innovative approach to balancing privacy with functionality.	Technical challenges in accurate human detection and blurring.
9	Stop recording when users are at home	Respects user privacy by limiting unnecessary recording.	Potential security gaps during transition periods.	Aligns with privacy trends in smart home technology.	Dependence on other systems (like WiFi) for functionality.
10	Use physical camera status indicator	Provides clear, immediate visual confirmation of camera activity.	Physical indicators can be tampered with or malfunction.	Increases user trust through transparent operational status.	Risk of false security if indicators are not perfectly synced with camera activity.
11	Physically isolate the camera when turned off	Enhances privacy by ensuring the camera is completely inactive.	Requires additional mechanical components and design considerations.	Strong selling point for privacy-focused users.	Potential mechanical failures or increased production costs.
12	Enhances privacy by ensuring the camera is completely inactive.	Requires additional mechanical components and design considerations.	Strong selling point for privacy-focused users.	Potential mechanical failures or increased production costs.	Risk of negative publicity and brand damage.

4.2.3 Advanced in-camera local video processing.

A considerable amount of ideas were proposed during the creative problem solving sessions to contribute to the formulation of this solution (see the following participant quotation):

PQ12: *"I think it might help if the data is stored locally and users have to access the data via local area network like the data will never go to any cloud server"*

PQ13: *"Maybe users can have the option to deploy it on their own server at home and store everything locally, so you don't have to even outsource it to your hardware"*

PQ14: *"Maybe the users can have settings like delete all clips that have human beings in the frame... And this is done locally. So that for devices like pet cameras that would be useful."*

Although the ideas from PQ12 and PQ13 are excluded, they are pointing to the same theme, that is to restrain recording and uploading by utilizing an embedded hardware system. Therefore, this solution relies on the ongoing enhancement of AI capabilities and the steady progression of computational power in embedded hardware systems. With the capability of in-camera local video processing, the feature of smart alerts can be implemented in-device rather than uploading footage to a cloud server.

The advantages of this solution are: (a) By focusing on utilizing in-device hardware, most of the uploading of footage can be avoided, which addresses the "concerns about the smart alerts feature" theme from the focus group result (see section 4.1.3). (b) It will not down-grade functionality of smart home monitoring devices in some use cases such as pet cameras, as human objects are not important in the use case.

The potential challenges of this solution are: (a) Current embedded hardware might not be capable of in-device object recognition tasks. (b) Even if the embedded hardware could do in-device processing, the result might not be as good as cloud-based processing. (c) The cost of such an embedded hardware solution might be too high for most products to apply.

4.2.4 Smart recording feature with extra information.

This solution is developed from an innovative idea proposed during the second creative problem solving session (See PQ15).

PQ15: *"This (Previous discussion) makes me think that maybe the camera could use some extra information to tell if the user is at home. For example, if the user's phone is connected to the Wifi network, that would mean the user is at home and for some use case, like mentioned by (another participant), pet camera, could totally work, I mean reducing many unnecessary recording."*

This solution connects smart home monitoring devices with other smart home products and personal devices. Optional configurations are provided to users so that if certain devices are active (e.g., smartphone connected to the Wifi network, certain lights are on), the device will stop recording.

The advantages of this solution are: (a) Avoid unnecessary recording based on rules founded by the user. (b) higher customization, which increases transparency, user control and user awareness.

The potential challenges of this solution are: (a)The configurations themselves have risks of being targeted, intruders may fabricate the extra information. (b) Balancing between intuitive design and complex configuration is challenging

5 Discussion and Limitations

5.1 Results of research

As shown in the results, the FG and CSP have both resulted in useful insights and more understanding of the perception of people. Based on the results from the focus group, it can clearly be stated that while people lack trust and comfort when using smart home monitoring devices they do see the value of convenience in them. The idea of misuse of data and lack of transparency having the users not know what happens with their data is what fears the participants. When it comes to considering smart devices, the convenience factor does seem to take priority as mentioned by most of the participants. If the results of the focus group were to be summarised, **"I think the convenience outweighs the risk, depending on the usage of the device"** as stated by one of the participants does a good job. Together with the scaling questions and the transcript of the focus groups a clear overview of the perception of people is established and the groundwork for the creative problem solving session is created.

However, there are still many factors, besides those mentioned in the focus group, that can be influenced to enhance the trust in smart home monitoring devices. Looking at the results from the creative problem solving session, 18 unique solutions were found of which 12 were eventually analysed to fit the scope of this research. The main factors mentioned by the participants in those solutions were: **Transparency**, as the participants provided many solutions that expect the companies to be transparent about their usage of your data, the protection of your data and how well the data had been protected. Secondly, the **tangible design** was a main theme of ideas. For instance, participants suggested different LED light colors, the direction of the camera, physical lens cap on/off to indicate the device status which allows people to easily tell whether is being recorded or not. Finally, in the **restraint recording and uploading**, participants propose ideas that use extra environment information such as identifying the owner's smartphone in the local network. By doing so the unnecessary recording can be avoided. Also, many ideas are about keeping data in local storage and avoiding unnecessary data uploading such as cloud-based object recognition. This can be interpreted as restraint recording and uploading, our solution of in-device processing and smart recording feature is based on these final factors.

5.2 Addressing the issue at hand

To link this all back to the questions proposed by this research, using the results from the focus group we can safely say that the perception of people is not positive when it comes to smart home monitoring devices. Where the feeling of comfort is not high when using smart home monitoring devices, due to the concern being high, which is mainly caused by the fear of the idea that something or someone could be misusing your data. The trust in smart home monitoring devices differs between people, but it can be said that none of the participants completely trust the smart devices with an integrated camera they own. However, due to the convenience of these devices, people are willing to take the risk while maintaining trust issues.

The creative problem solving session was intended to find solutions to enhance this trust, answering the second question. Looking at the 12 unique ideas gained from the creative problems sessions and analysing these considering the pros and cons, several solutions for various issues are found. Analysing these 12 ideas in the SWOT method allows for a clear overview to answer how to enhance the user's trust in smart home monitoring devices.

5.3 Limitations

The methods performed for this research are capable of showcasing a clear view of the perception of people concerning smart home monitoring devices. The issues and concerns, but also the positive sides are established by the discussions in the focus groups. Considering those issues, the creative problem solving session does well in providing several differing solutions for the issues that people seem to have with smart home monitoring devices. The problem, however, is that due to time constraints, the ability to generalise the outcome of this research is not achieved. With a lack of time, the amount of participants able to participate is too low to be of true scientific significance. This also leads to the idea that there might be some bias present in the perception of the participant population due to the convenience sampling. However on the other hand the perception of people is a very broad concept leading to very broad solutions, of which some are very unrealistic to achieve. Then considering the population of this research being mainly IT-oriented people, the expertise of these people fits perfectly for the scope of the research. Besides this limitation this does not mean that the research done is not of any significant value, the insights and solutions gained are still very creative and could be used as an inspiration for future research.

5.4 Future work

Something that would further the knowledge gained from this research would be evaluating the found solutions by use of a survey, allowing for a broader audience to evaluate the results from the smaller sample population. The idea of focusing on a larger scale is the way for future research, as the insights of other participants from different backgrounds would be even more informative. A very insightful population would be customers of certain smart home monitoring devices to compare their respective experiences with the same device, this would then coincide with the statement from the participant of our focus group where the weighing of convenience and concern depends on the usage of the device.

6 Conclusion

Smart home monitoring devices have evolved beyond their traditional security roles, gaining increased popularity with integrated camera features. However, this technological progress raises concerns about user privacy and data protection. The focus on these issues appears to be secondary, given the need for training data. Therefore the risk of accidentally capturing sensitive content increases. To address this, understanding people's experiences and concerns with these devices becomes crucial. Despite limitations in the sample population, this qualitative research is equipped to handle these questions. The research aims to answer the questions: "What are people's experiences, perceptions, and concerns regarding smart home monitoring devices?" and "How can trust in these devices be enhanced?" The focus group method revealed that distrust and concern are the primary issues with smart home monitoring devices. Users fear the misuse of collected data and lack of understanding of data handling, leading to low comfort levels in using these devices. However, convenience sometimes outweighs these concerns, causing users to accept the associated risks. The creative problem-solving session focuses on solutions for these issues, with participants suggesting transparency, tangible design, and limitations on recording and uploading as key improvements. These solutions, falling under the categories of awareness and control, are certain to enhance trust in smart home monitoring devices. Considering the SWOT analysis, these solutions could contribute valuable insights and serve as a foundation for future research. Additionally, they offer inspiration for companies and developers in the smart home monitoring device industry.

References

[1] Erin Beneteau, Yini Guan, Olivia K. Richards, Mingrui Ray Zhang, Julie A. Kientz, Jason Yip, and Alexis Hiniker. 2020. Assumptions Checked: How Families Learn About and Use the Echo Dot. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 4, 1, Article 3 (mar 2020), 23 pages. https://doi.org/10.1145/3380993

[2] Frank Bentley, Chris Luvogt, Max Silverman, Rushani Wirasinghe, Brooke White, and Danielle Lottridge. 2018. Understanding the Long-Term Use of Smart Speaker Assistants. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 3, Article 91 (sep 2018), 24 pages. https://doi.org/10.1145/3264901

[3] Federal Trade Commission. 2023. FTC Says Ring Employees Illegally Surveilled Customers, Failed to Stop Hackers from Taking Control of Users' Cameras. https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users. Accessed: 2023-12-06.

[4] Eileen Guo. 2022. A Roomba recorded a woman on the toilet. how did screenshots end up on Facebook? https://www.technologyreview.com/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy/. Accessed on January 15, 2024.

[5] Neilly H. Tan, Richmond Y. Wong, Audrey Desjardins, Sean A. Munson, and James Pierce. 2022. Monitoring Pets, Deterring Intruders, and Casually Spying on Neighbors: Everyday Uses of Smart Home Cameras. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (<conf-loc>, <city>New Orleans</city>, <state>LA</state>, <country>USA</country>, </conf-loc>) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 617, 25 pages. https://doi.org/10.1145/3491102.3517617

[6] Google Inc. [n. d.]. Set up and use Activity Zones. https://support.google.com/googlenest/answer/9207697?hl=en. Accessed on January 15, 2024.

[7] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. 2019. Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies* 2019, 4 (2019).

[8] TJ OConnor, William Enck, and Bradley Reaves. 2019. Blinded and Confused: Uncovering Systemic Flaws in Device Telemetry for Smart-Home Internet of Things. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks* (Miami, Florida) *(WiSec '19)*. Association for Computing Machinery, New York, NY, USA, 140–150. https://doi.org/10.1145/3317549.3319724

[9] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 65–80. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng

Appendix A: Protocol for Focus Groups

Preparation

- Prepare materials and tools for each participant, including post-it notes in two colours, pen, papers, information sheet (see appendix D), and consent form (see appendix G)
- The focus group is organized in the lecture room. We use two tables with refreshments, drinks, a laptop, and a microphone in the middle of the desk.
- Welcome participants, introduce ourselves, thank them for their participation and make them feel comfortable

Opening the focus group

- Introduce the topic and ask participants to fill out the consent form.
- The script of the opening is:
  Hello and welcome, we have gathered here today to conduct a focus group where we have invited students from the Human-Computer Interaction programme. The topic of today considers the usage of smart devices using integrated cameras at home. Before we start we would like to ask you each if you consent to participating in our research and you consent to this session being recorded. The consent form should be right in front of you.

Question List Before Break

- Question 1 (Opening question): Please Introduce yourselves and state whether you own a smart device besides a phone, and if so, which it is.
- Before continuing to ask questions, show participants use cases of smart home devices with images. The selected use cases include using pet cameras, baby monitors, and smart doorbells.
- For each following question, make sure to keep eye contact with all participants and confirm that everyone has said what they want to say before moving on to the next question.
- Question 2: Could you write down why you are in favour and against smart home monitoring devices in yellow and red post-it notes respectively?
- Question 3a: (After collecting participants' post-it notes) On a scale from 1 to 7, how would you rate the level of convenience of [the statement about why they are in favour of smart home monitoring devices in the collected post-it notes]
- Question 3b: (After collecting participants' post-it notes) On a scale from 1 to 7, how would you rate the level of comfort of [the statement about why they are in favor of smart home monitoring devices in the collected post-it notes]
- Question 4a: (After collecting participants' post-it notes) On a scale from 1 to 7, how would you rate the level of concern of [the statement about why they are against smart home monitoring devices in the collected post-it notes]
- Question 4b: (After collecting participants' post-it notes) On a scale from 1 to 7, how would you rate the level of trust of [the statement about why they are against smart home monitoring devices in the collected post-it notes]
- Question 5: Would you feel comfortable using a pet camera in your home? (With the image of the use case displayed on the screen of the laptop)
- Question 6: Would you feel comfortable using a smart doorbell in your home? (With the image of the use case displayed on the screen of the laptop)
- Question 7: Would you feel comfortable using a smart vacuum cleaner in your home? (With the image of the use case displayed on the screen of the laptop)
- Question 8: In what situation do you think another person might be able to see your camera's perspective?

Break

- Remind participants to help themselves with the refreshments on the table

Question List After Break

- Question 9: What factors, if improved, do you think will strengthen your trust regarding smart home monitoring devices? (If participants do not know where to start, we will provide three perspectives for reference: law and regulations perspective, technical perspective, and marketing perspective)
- For each factor mentioned in question 9, ask other participants what they think about that factor.

Closing the focus group

- One of the researchers who takes notes through the focus group session will briefly summarize what has been discussed. After that, we will ask participants if they want to correct any statement in the summary or if they want to add anything after listening to the summary.
- Thank participants again and ask them if they have any questions about the focus group.

Appendix B: Revised Protocol for Creative Problem Solving

Preparation

- Prepare a marker, large-size post-it notes, information sheet (see appendix F) and consent form (see appendix G) for each participant. We expect participants to write on the post-it notes using the marker, therefore large-size post-it notes are needed.
- The creative problem solving session is organized in the lecture room. We use one of the whiteboards in the lecture room. Researchers are standing beside the whiteboard and participants are expected to stand around the whiteboard as a circle.
- A microphone is held by one of the researchers.
- Welcome participants, introduce ourselves, thank them for their participation and make them feel comfortable

Problem introduction

- Explain what a smart home monitoring device is and give some examples.
- Ask participants to introduce themselves and state whether they own a smart device besides a phone, and if so, which one it is.
- We mention people's concern about using home monitoring devices and an example of data breaching incidents. We then state the question that we hope participants will solve.

Idea generation

- Ask the participants to start thinking about ideas and solutions to the problem. Participants should write down their ideas in the post-it notes, preliminarily categorize the ideas and stick them on the whiteboard.
- If any two post-it notes are related, we will reorganize the post-it notes to make sure they are close to each other.

Story Excursion

- When new ideas stop coming up, we will organise a story excursion
- For a story excursion, we give the first sentence of a story. We then require each participant to come up with another sentence that has a twist of the story. There are two rounds of storytelling among participants.
- After the excursion, we ask the participants to continue thinking about ideas.

Participant evaluation

- Each participant has three votes for their favourite ideas.
- Summarize the result and ask participants if they have anything to add or have any questions about the creative problem solving session.
- Thank participants again.

Appendix C: Information Sheet for Focus Groups

Is the internet watching your cat? - A qualitative research on trusting smart home monitoring devices

Information Sheet for Participation in the Study

How to consolidate the trust between people and smart home monitoring devices?

The aim of this research is by having students of the human computer interaction program find problems with smart home monitoring devices. After stating those problems, the participants are then used to create solutions for these problems established considering trusting smart home monitoring devices.

Purpose of this focus group is gaining useful insights of the students' perception considering smart monitoring devices. The focus group's goal is mainly establishing problems and starting with thinking towards solutions for them.

Procedure of the focus group follows the following structure:

1. Introduction to the topic
2. Familiarising and prior knowledge
3. Problem discovery
4. Solution
5. Evaluation

Any materials produced in the group may be used for publication but will be fully anonymised. An audio recording of the session will be taken (if you consent to it) and notes made.

Taking part in the focus group is voluntary and is not required for the course. You may withdraw from the focus group at any time for any reason.

If you have any queries, ask the researchers or email y.chen40@students.uu.nl

In case of any issues, please contact the course coordinator Prof. Masthoff

Appendix D: Information Sheet for Creative Problem Solving

Is the internet watching your cat? - A qualitative research on trusting smart home monitoring devices

Information Sheet for Participation in the Study

How to consolidate the trust between people and smart home monitoring devices?

The aim of this research is by having students of the human computer interaction program find problems with smart home monitoring devices. After stating those problems, the participants are then used to create solutions for these problems established considering trusting smart home monitoring devices.

Purpose of this creative problem solving session is gaining useful insights of the students' perception considering smart monitoring devices. The creative problem solving session's goal is mainly establishing problems and starting with thinking towards solutions for them.

Procedure of the focus group follows the following structure:

1. Introduction to the problem
2. Familiarising and prior knowledge
3. Problem discovery
4. idea generation
5. Evaluation

Any materials produced in the creative problems solving session may be used for publication but will be fully anonymised. An audio recording of the session will be taken (if you consent to it) and notes made.

Taking part in the focus group is voluntary and is not required for the course. You may withdraw from the focus group at any time for any reason.

If you have any queries, ask the researchers or email y.chen40@students.uu.nl

In case of any issues, please contact the course coordinator Prof. Masthoff

Appendix E: Consent Form

Is the internet watching your cat? - A qualitative research on trusting smart home monitoring devices

Consent Form for Participation in the Study

Please complete the form below by ticking the relevant boxes and signing on the line below. A copy of the completed form will be given to you for your own record.

□ I confirm that the research project ***"Is the internet watching your cat? - A qualitative research on trusting smart home monitoring devices"*** has been explained to me. I have had the opportunity to ask questions about the project and have had these answered satisfactorily.

□ I consent to the material I contribute being used to generate insights for the research project "***Is the internet watching your cat? - A qualitative research on trusting smart home monitoring devices".***

□ I am aware that the researcher will take an audio recording of the session. I understand that I can request to stop these recordings. I understand that I can ask for the recording to be deleted.

□ I understand that my participation in this research is voluntary, that it is not a requirement of my course, and that I may withdraw from the study at any time.

□ I consent to allow the fully anonymised data to be used for future publications and other scholarly means of disseminating the findings from the research project.

□ I confirm that I am 18 years of age or over.

□ I understand that the information/data acquired will be securely stored by researchers, but that appropriately anonymised data may in future be made available to others for research purposes only.

□ I understand that I can request any of the data collected from/by me to be deleted.

□ I agree to take part in the above study on ***"Is the internet watching your cat? - A qualitative research on trusting smart home monitoring devices"***.

Name of participant	Date	Signature
Name of researcher	Date	Signature