Folk Tales of IoT: Understanding the Impact of Stories on Users' Positive and Negative Perceptions of Smart Home IoT Devices

Leah Zhang-Kennedy
lzhangkennedy@uwaterloo.ca
Stratford School of Interaction Design and Business, University of Waterloo
Waterloo, Canada

Michaela Valiquette
michaelavaliquette@cmail.carleton.ca
Human-Computer Interaction, Carleton University
Ottawa, Canada

An Bella Chen
bella.chen@uwaterloo.ca
Cheriton School of Computer Science, University of Waterloo
Ottawa, Canada

Hilda Hadan
hhadan@uwaterloo.ca
Stratford School of Interaction Design and Business, University of Waterloo
Waterloo, Canada

Sangho Suh
sangho.suh@utoronto.ca
Department of Computer Science, University of Toronto
Toronto, Canada

ABSTRACT

This study examines how anecdotal stories from friends, peers, and online sources influence non-experts' perceptions and behaviors toward smart home IoT devices. We surveyed 263 participants, collecting narratives that either positively or negatively influenced their perception of IoT devices, which they retold in text and comic formats to encourage deeper reflection. Thematic analysis of the narratives, combined with quantitative survey data, reveals that stories significantly impact trust and willingness to use and adopt IoT devices. Negative stories, particularly those concerning security, privacy, and device unreliability, reduced trust and usage, while positive stories about home safety through monitoring and improved quality of life increased interest in IoT devices. Perceptions of different IoT devices varied based on the themes associated with the stories. The findings highlight the powerful role of storytelling in driving consumer acceptance of technology.

CCS CONCEPTS

• **Human-centered computing** → **Empirical studies in HCI**; • **Security and privacy** → *Social aspects of security and privacy*.

KEYWORDS

Smart Home, Internet of Things, Privacy and Security, Stories, Technology Acceptance, Mental Models, Folk Models

ACM Reference Format:
Leah Zhang-Kennedy, Michaela Valiquette, An Bella Chen, Hilda Hadan, and Sangho Suh. 2025. Folk Tales of IoT: Understanding the Impact of Stories on Users' Positive and Negative Perceptions of Smart Home IoT Devices. In *CHI Conference on Human Factors in Computing Systems (CHI '25), April 26-May 1, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/3706598.3713712

CHI '25, April 26-May 1, 2025, Yokohama, Japan

ACM ISBN 979-8-4007-1394-1/25/04…$15.00
https://doi.org/10.1145/3706598.3713712

1 INTRODUCTION

"WHY DID MY ALEXA JUST LAUGH OUT OF THE BLUE?!?!?!?" a user wrote on Twitter, "there's a good chance I get murdered tonight" another joked [34]. A survey conducted by Consumers International and the Internet Society found that up to 63% of consumers find connected devices (mostly smart home IoT devices) "creepy", and 53% said that they do not trust devices with their privacy. People's perception, trust, and technology practices can be influenced by first-hand personal experiences or stories they hear from other sources, such as news, media reports, social media, and through social connections [14]. Smart home IoT devices, such as voice assistants, thermostats, lights, cameras, door locks, and appliances, are unique from technologies like mobile devices and personal computers because they are embedded in the intimate, private spaces of the home and are often shared by household members and incidental users, such as guests. This shared usage creates complex dynamics around access, control and data management, which heightens concerns related to privacy, security, trust, and usability [2, 15, 37, 47, 57]. Previous research suggests that various factors influence consumer acceptance of IoT, including performance, user effort, social influence, hedonic motivation, and privacy and security [3]. However, it is not clear what types of stories people hear about these experiences and how the stories, accurate or not, influence their perception and behavior toward IoT adoption and management. In this research, we seek to understand: *What kinds of stories do people hear about smart home IoT devices?*; and, *How do these stories positively and negatively influence people's perception of IoT devices and their related practices?*

We use the term *folk tales* to refer to stories that laypeople know about technology that they have heard from other people. Often, product attributes may not be the only factor that evokes positive and negative consumer perceptions of technology; stories and images that circulate on social media, news, word of mouth, and popular culture can strengthen or undermine consumers' relationship with technology brands and provoke their adoption or rejection [24].

Our methodological approach is inspired by previous research that explored stories as information lessons to learn about security concepts [18, 41, 44]. Users often rely on over-simplified mental models to make decisions about online risks [53] based on what they learn from anecdotal stories shared by other people [41, 44], which could influence people's thinking and behavior. We seek to understand whether similar effects are observed for IoT technology, focusing on whether stories shared by other people that highlight negative and positive experiences influence the story recipients' trust and willingness to use IoT devices, even if they may not have personally experienced similar incidents.

We employed a novel approach by combining two established elicitation methods to collect narratives in both textual and visual formats, recognizing that each modality can reveal unique aspects of user perceptions, capturing nuances the other might miss [48]. Sketching as a data collection method has been shown to be effective in helping participants articulate abstract concepts and reveal their mental models, particularly in areas such as privacy [39], cybersecurity [48], web security [20], and understanding how complex systems work (e.g., Internet [29]). The duel data collection method acknowledges that Doppelgänger brand images—disparaging images and stories about a technology or brand that are circulated in popular culture—include both visual and textual representations [24]. Furthermore, narrative research suggests that inviting participants to use multiple types of texts—visual and written—can "serve both participants and researchers in gaining a richer and more complex understanding of participants' experiences and generating new perspectives and knowledge" [30]. Visual narratives, in particular, could surface "user mental models not uncovered via written and verbal articulation" [48].

In this work, we conducted an online survey to collect stories that people have heard about smart home IoT devices. Each participant self-selected a story that have positively and negatively influenced their perception and attitude towards IoT devices, and retold the story as text and visual narratives using an online drawing tool. Through thematic analysis of 263 pairs of text and comic narratives about IoT, we found that anecdotal stories, significantly shape user perceptions and behaviors. Negative stories, particularly those involving hacked devices, privacy risks, and unreliability, tend to have a more immediate and pronounced impact, eroding trust and deterring adoption. Positive stories, by contrast, often highlight home monitoring benefits and daily life enhancements, fostering greater interest and willingness to adopt IoT technology. Perceptions also varied by device type. For example, home security systems were predominantly associated with positive experiences, while voice assistants were more commonly associated with negative ones. Finally, we emphasize the role of emotional responses, such as anger, frustration, inspiration, and excitement, in mediating these effects.

This research makes three main contributions. First, we provide the sole empirical investigation into how "folk tales" circulate among laypeople influence trust, adoption, and willingness to use smart home IoT devices. Almost half (43%) of the participants reported changes in behavior after hearing these stories, suggesting that folk tales are powerful drivers of consumers' perceptions of technology. We suggest that researchers, IoT developers, and marketers can learn valuable lessons from these seemingly mundane, and sometimes weird and absurd stories that consumers associate with technology and address them in product design and communication strategies to foster consumer trust.

Second, we provide a comparative analysis of IoT experiences by examining both positive and negative narratives. While prior research has largely focused on risks such as privacy and security concerns, the positive aspects (e.g., enjoyment, convenience) have received less attention. Our study highlights how these contrasting narratives shape user perceptions and behavior. We found that negative stories exert stronger immediate effects, consistent with negativity bias, but positive stories can foster long-term enthusiasm and adoption.

Third, we demonstrate the value of the dual data collection method that combines textual and visual storytelling. This approach provides a rich, multidimensional understanding of user perceptions, as visual narratives reveal emotions, actions, and symbolic representations that text alone could not capture. We share insights from our experience of using this method and provide best practices for future researchers who employ this approach. Our dataset of IoT "folk tales" is publicly available[1] under a Creative Commons license[2], offering opportunities for further exploration.

2 BACKGROUND AND RELATED WORK

2.1 Stories Form Mental Models

Folk theories are beliefs and ways of understanding that help people interpret phenomena in everyday experiences [22]. Folk theories are often used to study users' understanding of how technology works because many inner workings of technology are hidden black boxes that hinder understanding of the details of their functionality [16, 43]. Users' interaction with technology in the home environment, from adjusting the heating with home thermostats [31] to setting the cooling temperature of refrigerators [38], is almost entirely understood through folk channels because people often do not learn about them through formal education [31]. Folk theories are sometimes called folk models, or mental models, which are often incomplete or inaccurate, but nonetheless help users reason about technology and influences their choices and decision making regarding those technologies [53].

Previous research [17, 41, 44, 53] suggests that users frequently encounter folklore in the form of security advice, word-of-mouth stories, and technology myths propagated in popular media. One focal area of the research area is on how people's security mental models are shaped in part by entertainment media [5, 21], such as fictional portrayals of computer security and hacking [25]. This phenomenon is observed in other fields, such as the effect of stories in popular media that can influence how people perceive health information [51]. Although there are some concerns about the potential spread of inaccurate and harmful misinformation, the imperfect presentation of medical stories in popular media had positive effects on people general medical knowledge [27]. Similarly, there is also strong evidence that people form their mental models of online threats based on reasoning about information from informal

[1] https://iot-storytelling.github.io

[2] Comics and text narratives created by the participants are licensed under CC BY-NC-ND 4.0, https://creativecommons.org/licenses/by-nc-nd/4.0/

stories told by other people, which could affect security and privacy-relevant decisions [41, 44, 53]. Inspired by these previous research, we explore the relationship between anecdotal stories and users' risk perception and practices toward smart home IoT devices.

2.2 Stories Influence Technology Practices

In terms of what characteristics of stories that could influencing users' thinking and behavior, Fassl et al., [17] suggests that security folklore could be mainly formed from normative beliefs based on social proof rather than behavioral beliefs (i.e., purpose and effects of security practices). Rader et al. [44] discovered that narratives containing significant threats have an impact on cognitive processes and the probability of being recounted. Redmiles et al. [46], found that the primary origins of security advice are unpleasant incidents that participants have personally encountered or learned about from friends, family, and the media. Fennell et al. [18] discovered that narratives about security breaches heightened individuals' likelihood to embrace certain security practices, such as two-factor authentication. Based on this evidence in supporting the influence of stories, we hypothesize that people also gain a significant amount of their knowledge about smart home IoT technology from stories they hear from family, peers, social networks, news, and entertainment media. However, it is unclear what kinds of stories people hear about IoT and how these stories influence their perceptions toward the technology.

Although previous work [41, 44] had shown that stories people hear from others impact their perception of security and related behavior, the focus was mainly on stories of negative experiences related to cybersecurity threats that had impacted security decision-making. For example, Rader et al. [44] found that stories with serious threats affect thinking and the likelihood of retelling. Redmiles et al. [46] found that the main sources of security advice come from negative events that the participants had personally experienced or had been shared by peers, family, and the media. Fennell et al. [18] found that stories about security breaches increased people's willingness to adopt two-factor authentication. They hypothesized that focusing on the negative consequence might encourage more adoption than communicating the benefits. In our study, we explored both the perceived benefits and risks people associate with smart home IoT by collecting stories that had negative and positive influences on our participants thinking and practices to identify what aspects of the stories they found compelling.

2.3 IoT Adoption and Usage in Smart Homes

Several factors influence the adoption and use of IoT devices in the context of the smart home [36]. Aldossari et al. [3] found that user expectations of the device's performance, ease of use, social influence, price value, and enjoyment and pleasure of using the technology are significant predictors. They also found that security risk and trust also play a significant role in the acceptance of smart home. Tan et al. [26] investigated the privacy and security tensions that arise between primary users and other stakeholders based on how people use smart home cameras to monitor and surveil in homes and neighborhoods. Due to the internet-connected nature of IoT products and services, there is an increased risk of data security and privacy breaches, often without the knowledge of the user [8]. Therefore, previous research had explored users' privacy perceptions and concerns with smart home technology [37, 56, 57] and specific types of devices, such as smart speakers with voice assistants [33], smart meters [28], smart cameras [6], and connected toys [35]. Users are particularly concerned about information sold to third parties or when devices lack access control, which could increase their perceived risks and decrease their desire to purchase the device [15]. Users seem more comfortable with data collection in public spaces than in private spaces [37], and devices such as voice assistants are often placed in a central and shared location at home [33]. Households inhabitants can play various roles in the planning, setup, usage, and maintenance of smart homes [36]. Therefore, the privacy preferences of a variety of user types should be considered, such as bystanders and non-primary users [1, 6, 50, 55], older adults [23], children [35], and power users [40]. Although we revisit some of the themes related to risks and concerns from previous research, our primary focus is on how incidents, as shared through stories told by others rather than personal experiences, influence recipients' perceptions of risks and practices.

2.4 Visual Elicitation Methods and Analysis

Sketching offers additional insight into experts and non-experts' conceptualizations of abstract concepts that are difficult to express with verbal and textual information alone [7, 11]. Sketching has been used to identify experts and non-experts' mental models of the internet [29], people's general understanding of privacy [39] and cybersecurity [48], and users' understanding of web security [20]. The drawing method was also used to study vulnerable populations like older adults (e.g., [45]) and children (e.g., [39]), who might have difficulty articulating technical concepts through words alone. Visual data from drawings and diagrams also help researchers improve the design of computing systems, such as home network management tools [42], and aid in the design of privacy tools and mechanisms [39, 54]. Most sketch elicitation methods have traditionally relied on free-form pen-and-paper drawings. However, some researchers have developed digital tools to create visual content [49]. While there has been various research on using sketching to elicit users' perceptions of online risks, no study has combined visual and textual narratives to explore these perceptions. Integrating both approaches could provide complementary insights into how users perceive the risks and benefits of smart home IoT technology.

3 METHODOLOGY

3.1 Data Collection

We conducted an online survey, approved by our institution's Research Ethics Board (REB), using Qualtrics and distributed through Prolific[3]. The survey featured various question types (e.g., Likert-scale, multiple choice, short answer, drawing task), organized into five main sections. This structure was designed to minimize the cognitive load and encourage participants to reflect more deeply on the stories they encountered. The detailed survey questions can be found in Appendix A.

3.1.1 Survey Design.

[3]https://www.prolific.com

1. *Consent & Introduction.* During the consent process, we emphasized that participants would share anonymous stories about *other people* rather than personal experiences. This approach aimed to reach our goal of collecting anecdotal stories, but also helps reduce the social stigma associated with being a victim [4, 12] (since the stories are about other people) and minimize social desirability bias. To ensure that participants had a baseline understanding of IoT devices in home settings, we provided a brief explanation with various device examples and included an attention check question midway through the survey.
2. *Story Prompts.* We adapted story prompts used in previous work to enhance participants' ability to recall and share their narratives more effectively. [41, 44]. Participants first listed various stories they had heard about smart home IoT devices and selected one that they could easily recall in detail to share in the survey. Next, we asked participants to specify whether their chosen story had a *positive* or *negative* impact on their perceptions of IoT technology.
3. *Facts and Story Influence.* For their chosen story, participants answered questions about its source, the severity of the incident (if negative), their belief in its truthfulness, and their emotional reaction to the story. Next, participants rated the story's impact on their perceptions, trust, and willingness to use IoT devices using Likert scales.
4. *Retelling the Story.* To gain detailed insights into their thoughts and recollections, participants were asked to describe the story as if sharing it with a friend, family member, coworker, or acquaintance, then indicated the channel they would share the story, such as text messaging, email, social media, blog post, phone, or in-person. We did not impose a time limit for these tasks but recommended 15-20 minutes. Participants' stories were retold in two formats:
   - *Text:* Participants described the story in a text box provided in the survey.
   - *Comic:* Participants completed the drawing task using a web-based comic authoring tool developed by us[4] from the open-source drawing tool Excalidraw. The tool provided basic drawing support, allowing participants to easily create, download, and upload finished comics into the survey. It supported free-form drawing with a pen tool, customizable shapes, colors, strokes, and fills. To streamline the process for those with no previous drawing experience, participants could access an optional library of pre-made graphical components, such as comic panels, speech bubbles, stick figures, and icons representing common smart home IoT devices. Participants also provided brief captions for their comics to help researchers accurately interpret their drawings.
5. *Demographics Information.* The survey ended with questions about participants' previous experience using IoT devices and demographic information.

3.1.2 Testing the Survey and Drawing Tool. We pilot-tested the survey and drawing tool with 63 undergraduate students who received the survey as an in-class activity during a lecture on smart home IoT. Based on the completed survey responses, the drawing output, and the qualitative feedback, we improved the clarity of the survey questions and the instructions for the drawing task.

3.1.3 Participant Recruitment. We recruited 300 participants from North America on Prolific. We applied a gender quota during recruitment to obtain a representative sample of populations in the United States [52]. The average survey completion time was 34 minutes ($Md = 29$) and the participants were remunerated 5 GBP. 37 responses were discarded due to data quality issues, failure to correctly answer the attention check question, or incomplete responses (e.g., failed to upload a drawing). A total of 263 responses were retained for data analysis after quality checks.

3.1.4 Participant Demographics. The participants' demographics information is summarized in Table 1. Our sample is representative by gender but not by age, where the majority (91%) of the survey participants are between 18 and 54 years of age. Most of our participants (79%) do not have a technical background. 91% owned at least one IoT device, with 78% owning multiple devices. Smart media devices (75%), voice assistants (58%), wearables (49%), smart appliances (45%), home security systems (27%) are the most widely used types of devices.

3.2 Qualitative & Quantitative Data Analysis

We used a combination of qualitative analysis to identify patterns in the stories and statistical analysis to assess how the stories impacted attitudes and behaviors toward IoT device adoption and usage.

3.2.1 Thematic Analysis. We used inductive thematic analysis [10] to analyze written stories and illustrated comics. The goal is to ground our analysis in the data to identify reoccurring patterns and themes as they emerge from the data.

Code Development and Reliability. A research assistant (RA1) experienced in qualitative analysis reviewed all open-ended responses to become familiar with the data by reading and re-reading the responses to gain a comprehensive understanding and writing down notes of preliminary observations of potentially significant elements in the data. RA1 then open-coded a subset of 30 open-ended responses (11% of the data) in Atlas.ti. RA1, along with two senior researchers, discussed and refined the open codes to develop an initial codebook. A second research assistant (RA2), who was familiar with the data but not involved in code development, independently analyzed the same subset using the codebook. In the first round, the two coders met to discuss their coding strategies and collaboratively refined the codebook. In the second round, RA1 and RA2 recoded the data based on the updated codebook. An inter-rater reliability test using Krippendorff's alpha coefficient [32] showed good agreement between the two coders, $\alpha = 0.87$[5]. The two coders discussed and jointly resolved the remaining disagreements.

Using the refined codebook, the RA1 coded the remaining survey responses, meeting weekly with the research team to make minor adjustments until all open-ended questions were coded. To identify the type of stories told, we organized the codes into two categories on the Miro visual whiteboard platform: one for stories that had a positive influence and another for those that had a negative influence on participants' perceptions toward IoT devices. The

[4] https://privacytoon.uwaterloo.ca/projects/create/

[5] Krippendorff [32] suggests that $\alpha \geq 0.823$ is a good agreement.

Table 1: Participant demographics. Gender and age are compared to US census data [52], shown in brackets.

Gender		Age		Education Level		Devices Owned	
Man	50% (49%)	18–24	12% (~9%)	No high school	1%	Smart media devices	75%
Woman	50% (51%)	25–34	33% (14%)	High school	27%	Voice assistants	58%
Non-binary	2% (-)	35–44	29% (13%)	College	12%	Wearables	49%
Prefer not to say	<1% (-)	45–54	17% (12%)	Bachelors	46%	Smart appliances	45%
		55–64	6% (13%)	Masters	15%	Home security systems	27%
		65–74	2% (10%)	Doctoral	3%	Medical health monitors	10%
		Prefer not to say	<1% (-)	Prefer not to say	<1%	Smart toys or baby monitors	10%
				Other degree	1%	Other	6%
						don't own an Iot Device	9%

research team then collaboratively developed themes within these categories, discussing and refining them until reaching consensus.

Triangulation of Textual and Visual Data. We used two data sources, text and comics, in our data analysis to develop a more comprehensive understanding of people's perception of IoT devices. We created 143 codes for the text narratives and 157 codes for the comic narratives. Table 2 shows an example top-level code category, `Coda`, which describes a story's conclusion and the characters' reactions to the events in the story. `Gets-Rid-of-IoT` is an second-level code related to the category. We created the code strings `Coda_Gets-Rid-of-IoT.txt` for text narratives and `Coda_Gets-Rid-of-IoT.comic` for comics. We created 14 additional codes for the comic narratives to capture unique visual elements, such as symbols and characters. For example, the top-level category `Emotion` and the related codes are used in both formats to capture characters' feelings, but codes related to the category `Emotional-Signs` are only used for comics to capture graphical elements like emojis. Our goal is to triangulate relationships between coded text and their visual counterparts across the two formats. The comic and text dataset are organized thematically according to the types of stories summarized in subsection 4.4.

3.2.2 Statistical Analysis. First, we conducted a between-group analysis to compare the willingness to use and trust in IoT devices between participants who heard positive stories versus those who heard negative stories. We used Wilcoxon rank-sum tests [19] with Bonferroni correction [9]. Next, we followed-up with a series of regression analyses to identify factors that influenced participants' behavior and attitude changes as a result of hearing the story. We used participants' self-reported responses for behavior change, willingness to use, and trust towards IoT devices as dependent variable (DV). Following the approach in the literature [41, 44], we employed logistic regression for the binary DV and Ordinary Least Squares (OLS) regression for interval-scaled DVs in R[6]. Factors such as perceived story characteristics, beliefs, and demographic information are used as predictors (see Table 3).

In reporting our findings, we use monospace font for variable names to improve clarity (e.g., `behavior_change`). We report only predictors that showed statistical significance (i.e., $p < .05$) in the regression analyses, summarized in Table 7, Table 8, and Table 9. Our study is the first to explore how factors from anecdotal stories influence people's behavior and willingness to use, and trust towards IoT devices. To establish a baseline understanding of the unique influence of each factor, we assume that each predictor independently affects the DVs. Thus, we employed univariate regression models, each using a single factor as the predictor, to isolate and quantify the independently influences of each variable to the DV.

Behavior. To explore factors influencing participants' likelihood of behavior change after hearing a story, we used their self-reported responses (Yes, No, Other) to the question, "Did you start doing anything differently after hearing the story?" (`behavior_change`) as the dependent variable. Given that these responses do not follow a sequential order, we further re-coded the "Other" responses ($n = 12$) as "Yes" in our regression analyses, as these participants indicated that they had seriously considered changes, such as removing their IoT devices, but had not yet acted on them. To validate this approach, we conducted regression analyses both with and without recoding the "Other" responses, finding no significant differences. Thus, we present the results with the re-coded responses to maintain a full dataset. We then conducted a series of single-predictor logistic regressions to identify factors associated with behavior change. We report the results in Section 4.6.1.

Perception. To assess changes in participants' perceptions towards IoT devices, we inquired about participants' trust in and willingness to use IoT devices. We considered variations in these two variables as indicators of perception change. We began by analyzing participants' responses to the 5-point Likert-scale questions. For those who selected stories that they felt negatively influenced their perception, we asked: "How much do you think hearing this story has *negatively* affected your *trust* towards IoT devices?" For participants who selected a story they believed had a positive impact, we asked: "How much do you think hearing this story has *positively* affected your *trust* towards IoT devices?" These responses were used as the dependent variables, `neg_story_trust_change` and `pos_story_trust_change`, respectively, in our single-predictor linear regression analyses in Table 8 of the results. We then analyzed participants' responses to the 5-point scale questions regarding their willingness to use IoT devices after hearing the story. For those who shared stories that they believed to have a positive impact, we asked: "How much do you think hearing this story has *positively* affected your *willingness to use* IoT devices?". For those

[6]R package — glm: Fitting Generalized Linear Models. https://www.rdocumentation.org/packages/stats/versions/3.6.2/topics/glm; ols: Linear Model Estimation Using Ordinary Least Squares. https://www.rdocumentation.org/packages/rms/versions/6.8-1/topics/ols

Table 2: A subset of codes used in the open coding process in Atlas.ti. The codes are grouped based on the axial coding process in the format "Category_Code". Both text and comic data are coded with related codes to enable triangulation during analysis. For instance, text data is labeled with `.txt` (e.g., `Coda_Buys-More-IoT-Devices.txt`), while visual data is labeled with `.comic` (e.g., `Coda_Buys-More-IoT-Devices.comic`)

Category_Code	Description
Coda_Buys-More-IoT	decides to buy an IoT device or more IoT devices
Coda_Gets-Rid-Of-IoT	decides to get rid of their IoT device(s)
Coda_No-Change	no change in behavior and does not do anything differently based on the story
Coda_Share-Story	reports the story online (e.g., social media) to "warn" or "persuade" others about risks or benefits
Coda_Unplugs-Device	unplugs the device(s) due to degraded trust towards the device, but still occasionally use the device
Coda_Will-Not-Purchase	refuses to buy an IoT device or more IoT devices

Table 3: Dependent variables, predictors, and their corresponding survey questions in our regression analyses

Coded Name	Survey Questions Summary*
Dependent Variable	
behavior_change	Behavioral change after hearing the story–Q8. *(Yes/No/Other)*
pos_story_trust_change	†Positive story positively impacts trust in IoT devices–Q13a. *(1 = Not at all to 5 = A lot)*
neg_story_trust_change	‡Negative story negatively impacts trust in IoT devices–Q13b. *(1 = Not at all to 5 = A lot)*
pos_story_willingness_change	†Positive story positively impacts willingness to use IoT devices–Q14a. *(1 = Not at all to 5 = A lot)*
neg_story_willingness_change	‡Negative story negatively impacts willingness to use IoT devices—Q14b. *(1 = Not at all to 5 = A lot)*
Predictor	
vivid_recall	Story recall vividness–Q3. *(1 = Least vivid; 10 = Most vivid)*
time_since_story	Time since hearing/reading the story–Q4. *(from "Within the last day" to "Longer than three years ago")*
medium	Medium through which the story was heard/read–Q5. *(Multiple choice)*
source	Source of the story–Q6. *(Multiple choice)*
story_sentiment§	Story's positive or negative influence–Q7. *(Multiple choice)*
belief	Belief in the story's authenticity–Q10. *(Yes/No/Not sure)*
seriousness	Perceived seriousness of the threat/problem–Q11. *(1 = Not at all serious, 5 = Extremely serious)*
emotions	Emotions associated with the story–Q12. *(Multiple-answer multiple choice)*
demographic	Age, Gender, Education Level–Q25 to Q27. *(Multiple choice)*
pos_IoT_experience	†Personal positive experiences with IoT devices–Q24a. *(Yes/No)*
neg_IoT_experience	‡Personal negative experiences with IoT devices–Q24b. *(Yes/No)*
technical_Background	Formal training in a technical field–Q31. *(Yes/No)*

Note. We only report predictors that showed significance (i.e., $p < .05$) in the regression analyses in Table 7, Table 8, and Table 9.
†. Conditional questions shown only to participants who selected positive stories in Q7.
‡. Conditional questions shown only to participants who selected negatives stories in Q7.
§. This predictor was included only when the dependent variable is `behavior_change`, as other dependent variables were specific to either positive or negative stories.

who shared stories that had a negative influence, we asked: "How much do you think hearing this story has *negatively* affected your *willingness to use* IoT devices?" In Table 9 of the results, these responses were used as dependent variables in our single-predictor regression analyses, labels as `pos_story_willingness_change` and `neg_story_willingness_change`, respectively. We report the results in Section 4.6.2.

4 RESULTS

4.1 Story Facts

The text descriptions of the stories averaged 91 words, while the comics averaged 3 panels long. Among the comics, 67% were multi-panel, and 33% were single-panel. Most comics (87%) included both images and text, while 13% featured only images. Most of participants (80%) reported recalling the story details from fairly vividly to very vividly (7-10 on a 10-point Likert scale), and 93% had heard the story they shared within the last three years.

Participants self-identified the story they heard as having a positive or negative influence on their perception and attitude toward IoT devices. In the paper, we refer to these *positive stories* and *negative stories*. For clarity, we use the symbol (+) in the participant codenames and excerpts to denote the participants who shared positive stories and (−) for those who shared negative stories (e.g., $P137^{+}$, $P200^{-}$). As summarized in Table 4, 142 participants chose to share negative stories and 121 participants told positive ones.

4.1.1 Source & Medium. Figure 1a shows that stories heard from friends (31%), news institutions (20%), family (15%), and strangers

(15%) together account for 81% of the stories. Figure 1b shows that the stories came from a variety of sources, with in-person face-to-face conversations (41%), social networking sites (29%), and online news media sites (11%) being the most common. Most of the participants (94%) believed the stories to be true, 5% were not sure, and only 2% believed them to be false.

4.1.2 Events and Settings. Events that occurred in shared stories that were triggered, enabled, or exacerbated by IoT devices frequently included security and privacy threats such as hacking, targeted advertising, and surveillance. We also observed other physical security and safety incidents like break-ins, theft (e.g., Amazon package stolen), and injury detection (e.g., camera records accidental falls). However, several stories also described alarming social and criminal offenses such as harassment, domestic abuse, stalking, spying, blackmailing, and violent home intrusions. Most of the events took place at home, with the living room being the most mentioned space followed by the bedroom. Other events took place outside, but near the home, such as the entrance, porch, yard, street, or a neighbor's doorway. Only a few stories occurred in public spaces, such as a park or a school.

4.1.3 Affected Individuals. In the stories told, our participants portrayed various characters affected by incidents related to IoT. Female characters are more frequently portrayed as being affected by technology than male characters. The stories mainly involved single users, but also included families, couples, and vulnerable populations such as children, seniors, and disabled people. Sometimes, bystanders, such as care workers, neighbors and friends, and even pets, are also affected by IoT. Some stories involved supporting personnel on site as a result of interaction with an IoT device (e.g., call 911 on Alexa), such as police officers, paramedics, and other emergency response workers. The perpetrators described in the events are almost always men who were often strangers, employees, friends, or relatives. Non-gendered perpetrator entities included the government and IoT manufacturers.

4.2 Types of IoT devices Shared in the Stories

Most of the shared stories are about home security systems (42%) and voice assistants (30%). We also collected some stories about smart home utility devices (7%), smart toys and baby monitors (5%), smart appliances (4%), and wearables (3%). A small group of stories (10%) described general concerns about smart home devices but did not specify the type of device. Table 4 provides an overview of the types of devices featured in the stories.

4.2.1 Home security system. 42% (n = 112) of the participants shared stories about home security systems. The devices mentioned included sensors, cameras, and alarm systems that enable remote monitoring and control of home security via the the Internet. Examples include smart doorbell cameras like Ring, which allow users to access real-time data and video surveillance. The stories often expressed positive sentiments highlighting the benefits of these devices in monitoring unexpected risks. The characters in the stories installed cameras both inside and outside their homes, with most positive stories involving devices placed outside, such as surveillance cameras on entrances, porches, and yards to monitor activities in these specific locations. In contrast, negative stories often involved indoor devices, which raised privacy concerns or potential unauthorized surveillance by hackers.

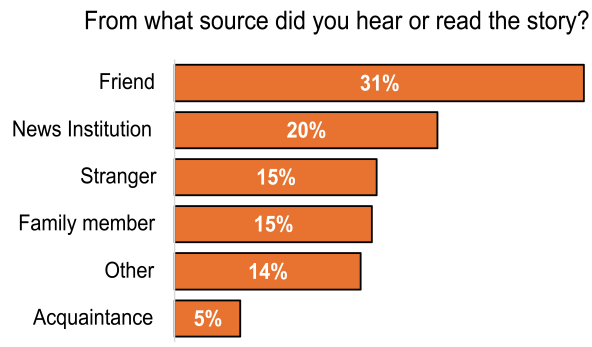
4.2.2 Voice assistant. 30% (n = 80) of the participants shared stories about intelligent virtual assistants that interact with users via voice commands, subsequently performing the corresponding tasks or providing information (e.g., Alexa, Echo). Most of these stories expressed negative sentiments, focusing on concerns about privacy, such as automatic data collection, unauthorized recording, and data sharing with third parties. However, about 26% of the stories highlighted the benefits of voice assistants, including their usefulness for entertainment (e.g., playing music), education (e.g., answering questions), and integration with other IoT devices to create a seamless smart ecosystem. Some stories described voice assistants as critical lifelines in emergency situations, such as making distress calls to 911 by voice command.

4.2.3 Smart home utility. 7% (n = 18) of the participants shared stories about home utility devices, such as smart thermostats, lights, and plugs. More than half reflected positive experiences, highlighting the benefits of remote activation and control, which improve efficiency, well-being, and potential cost savings. For example, P89^{+} described a person who installed a smart thermostat and experienced a significant reduction in energy bills, which led to a sense of satisfaction of being eco-friendly and saving money. In contrast, negative stories often involved malfunctioning devices, such as faulty temperature sensors that led to unexpected energy consumption and higher utility bills.

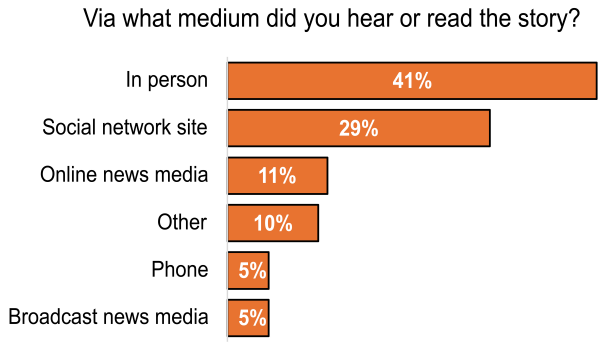
4.2.4 Smart toy and baby monitor. All stories about IoT toys and baby monitors were reported as negative experiences. 5% (n = 12) of the participants expressed universal concerns about these devices being vulnerable to hacking and the associated risks to children. The stories recounted instances where hackers used these devices to scare children, encourage misbehavior, and threaten families. Such experiences were deeply distressing for the individuals involved, leading our participants who heard these stories to pledge not to use similar products in the future.

4.2.5 Smart appliance. Stories about household appliances with smart features, such as smart refrigerators, smart TVs, and robotic vacuum cleaner, accounted for only 3% (n = 8) of the stories. Positive stories highlighted the usefulness of these devices and their seamless integration with other smart devices like voice assistants. In comparison, negative stories often focused on unexpected malfunctions, such as smart refrigerators making strange noises at night or robotic vacuums that run over and spread pet waste during an automated cleaning cycle.

4.2.6 Wearable. Another 3% (n = 8) of the participants shared stories about wearables, which are used to monitor and record personal health and activities. These devices included smartwatches, wristbands, headphones, and RFID and Bluetooth tags. In addition, two stories focused on specialized medical devices designed to track health data, such as smart heart monitors to help patients understand and manage their physical health conditions.



(a) Story Source. Note: The "other" category summarizes sources selected by 4% or fewer participants, which includes Coworker or Boss, IT or Computer Repair Person, and those who reported "Don't remember" or unspecified sources.



(b) Story Medium. Note: The"other" category summarizes mediums selected by 3% or fewer participants, which includes Email, Video chat, Text message, Print news media, Chat, Blog posts, and those who reported "Don't remember" or unspecified mediums.

Figure 1: Story Source & Medium

Table 4: Types of devices that the stories focused on that had negatively or positively influenced our participants' perceptions toward the devices.

Devices	Negative	Positive	Total
Home security system	14%	28%	42% (112)
Voice assistant	23%	7%	30% (80)
Smart home utility	2%	5%	7% (18)
Smart toys and baby monitor	5%	0	5% (12)
Smart appliance	1%	2%	3% (8)
Wearable	1%	2%	3% (8)
Unspecified	7%	3%	10% (25)
	54% (142)	46% (121)	100% (263)

4.3 Stories with Negative Influence on Perception

Slightly more than half (54%, $n = 142$) of the participants shared stories that they themselves identified as having negatively influenced their perception towards IoT. These stories fall into three main themes: 1) hacks, 2) tracking and spying, and 3) device unreliability. The sub-themes related to the main themes are presented in small caps in Table 5 and in-line (e.g., PROPERTY PROTECTION).

4.3.1 Hacks. Stories about hacked IoT devices made up 35% ($n = 92$) of the shared stories. While some stories expressed concerns about SECURITY VULNERABILITIES and hackers accessing PRIVATE INFORMATION, the most common stories involved VERABAL HARASSMENT from hacked voice assistants and baby monitors. These stories often described devices transmitting hateful messages, profanity, and threats intended to scare the occupants. A frequently shared story involved a stranger's voice delivered through a hacked baby monitor that scared children and their families, as shown in Figure 2a. Other incidents included FINANCIAL LOSS from unauthorized online purchases made by hacked smart voice assistants, and BLACKMAIL, where hackers demanded money from families to stop spying (Figure 2b).

Some stories are about SUSPECTED HACKS and the uncertainty surrounding them, where unusual behavior in IoT devices caused by technical problems is often mistaken for hacks [47]. For example, a common anecdote involves devices that unexpectedly play strange sounds, causing the occupants to suspect they have been hacked. P200^{-} shared:

> *At some point someone hacked into the Alexa device, or it just started to act erratically, and it would do a creepy laugh in the middle of the night. It also started making all kinds of weird noises, playing random songs out of nowhere, and answering questions it wasn't asked. It can really make you jump when it happens out of nowhere, especially in the middle of the night!*

Regardless of whether a hack is real or speculative, the stories generally emphasized psychological and emotional harm to the inhabitants, such as feeling "worried," "scared," and "creeped out".

4.3.2 Tracking. Around 9% ($n = 23$) of participants shared stories about unexpected DATA COLLECTION by IoT devices for PROFILING AND ADs. These stories often described smart voice assistants that continuously "listen and record" conversations, leading to the collection and analysis of this information, which then results in unexpected ADs. For example, Figure 2c illustrates a case where after discussing a luxury hotel stay with a friend, the characters

Table 5: Themes and sub-themes of the types of stories that participants had self-declared to have positively or negatively influenced their perceptions towards IoT devices. The numbers in brackets beside the themes and sub-themes indicate the frequency of occurrence out of 263 responses.

Themes	Sub-themes			
⊖ NEGATIVE (n = 142, 54%)				
Hacks (57)	VERBAL HARASSMENT (24)	SECURITY VULNERABILITIES (11)	SUSPECTED HACKS (7)	PRIVATE INFORMATION (6)
	BLACKMAIL (5)	FINANCIAL LOSS (4)		
Tracking (52)	DATA COLLECTION (26)	PROFILING & ADS (15)	SPYING OR STALKING (7)	GOVERNMENT SURVEILLANCE (4)
Unreliability (31)	ERROR PRONE (25)	COMPATIBILITY (6)		
Other (2)				
⊕ POSITIVE (n = 121, 46%)				
Home Monitoring (68)	PROPERTY PROTECTION (32)	EMERGENCY RESPONSE (19)	EVIDENCE (17)	
Enhance Daily Life (49)	USEFUL & CONVENIENT (26)	FUNNY MOMENTS (11)	CAREGIVING (8)	ENERGY SAVINGS (4)
Other (4)				

are bombarded with ADs for bedding products. This led to suspicion about their Alexa device and privacy concerns about the technology that enters one's home. Main concerns include data being transmitted to third parties without users' knowledge and consent, and devices placing unauthorized online purchases based on the owners' behavioral profile.

We received a small group of stories related to SPYING OR STALKING. These stories typically portrayed devices with recording and location-tracking capabilities being used to monitor and control others. The perpetrator is usually a person known to the victim, such as family members, ex-spouses, neighbors, or employers. Examples included spying parents on children's activities, intimate partner abuse, and employee location tracking. Other stories also raised concerns about GOVERNMENT SURVEILLANCE and control. For example, P259^{-} shared a story about a friend's worry that governments might mass access personal smart thermostats to control home temperatures for energy savings on a large scale during extreme weather conditions.

4.3.3 Unreliability. Around 19% (n = 49) shared stories about the unreliability of IoT devices. These devices, characterized as ERRORS PRONE, frequently malfunction and cause technical issues, which in turn erode user trust. Examples include Google Home that erroneously turns all lights on and off or sends error notifications about front doors being unlocked in the middle of the night. Some stories highlighted the devices' perceived lack of intelligence. For example, P42– shared a story (Figure 2d) about a friend who asked Alexa to play a radio station but found that the device repeatedly misunderstood the request despite various attempts.

4.4 Stories with Positive Influence

Just under half of the participants (46%, = 142) shared stories they felt positively influenced their perception of IoT. These stories fall into two main themes: 1) safety enabled by home monitoring, and 2) enhance daily life.

4.4.1 Home Monitoring. Many of the stories clearly communicated the perceived benefits in using devices like cameras and recording equipment to protect personal property and improve safety. Approximately a quarter of the participants shared stories about monitoring, such as doorbell cameras to deter potential intruders. Although the specifics of these events varied, IoT devices consistently played a significant role in PROPERTY PROTECTION. For example, P253^{+} recounted a story heard from a neighbor that their smart doorbell camera successfully prevented a potential burglary (see Figure 3a)

Several stories highlighted the EMERGENCY RESPONSE capabilities of IoT devices such as wearables, medical health monitors, and cameras, especially for infants and the elderly. These devices alert users to abnormal readings, potentially preventing life-threatening situations, such as heart attacks, fires, physical injury (e.g., falls), child abuse, and domestic violence. Often, these devices are purchased for other purposes, with emergency response being an unexpected but valuable benefit. Additionally, recordings from IoT devices served as crucial EVIDENCE in investigating misconduct and crimes. For example, P112^{+} told a story in which a doorbell camera recording helped solve a hit-and-run case: *"the police were able to use the ring doorbell video to identify the driver and bring him to justice."* In summary, these stories highlight how IoT devices enhance home monitoring through alerting, recording, and reporting, thus improving personal safety and potentially saving lives in emergencies.

4.4.2 Enhance Daily Life. Stories frequently emphasize how IoT devices enhance various aspects of domestic life. The theme of USEFUL & CONVENIENT emerged often in the stories, with evidence of deep appreciation for smart automation features. These include cleaning, setting timers and reminders, remote control, multitasking, improving well-being, and even parenting. For example, P123^{+} described several benefits a family experienced:

> *…I saw a woman [on TikTok] ask Alexa to tell her kids it was bedtime and they listened! I saw her put a timer on for how much longer her son could be on the ipad, and when the timer went off, he stopped playing with the iPad. She was able to turn on/off the Christmas Tree lights, the outside lights. The Alexa could start her vacuum cleaner robot (which I also bought because of TikTok videos!) One of the best parts was the jokes that Alexa could tell her kids, that her kids could request music to listen to, or even call Santa. This device was shown to be fun and life changing for her and her family.*

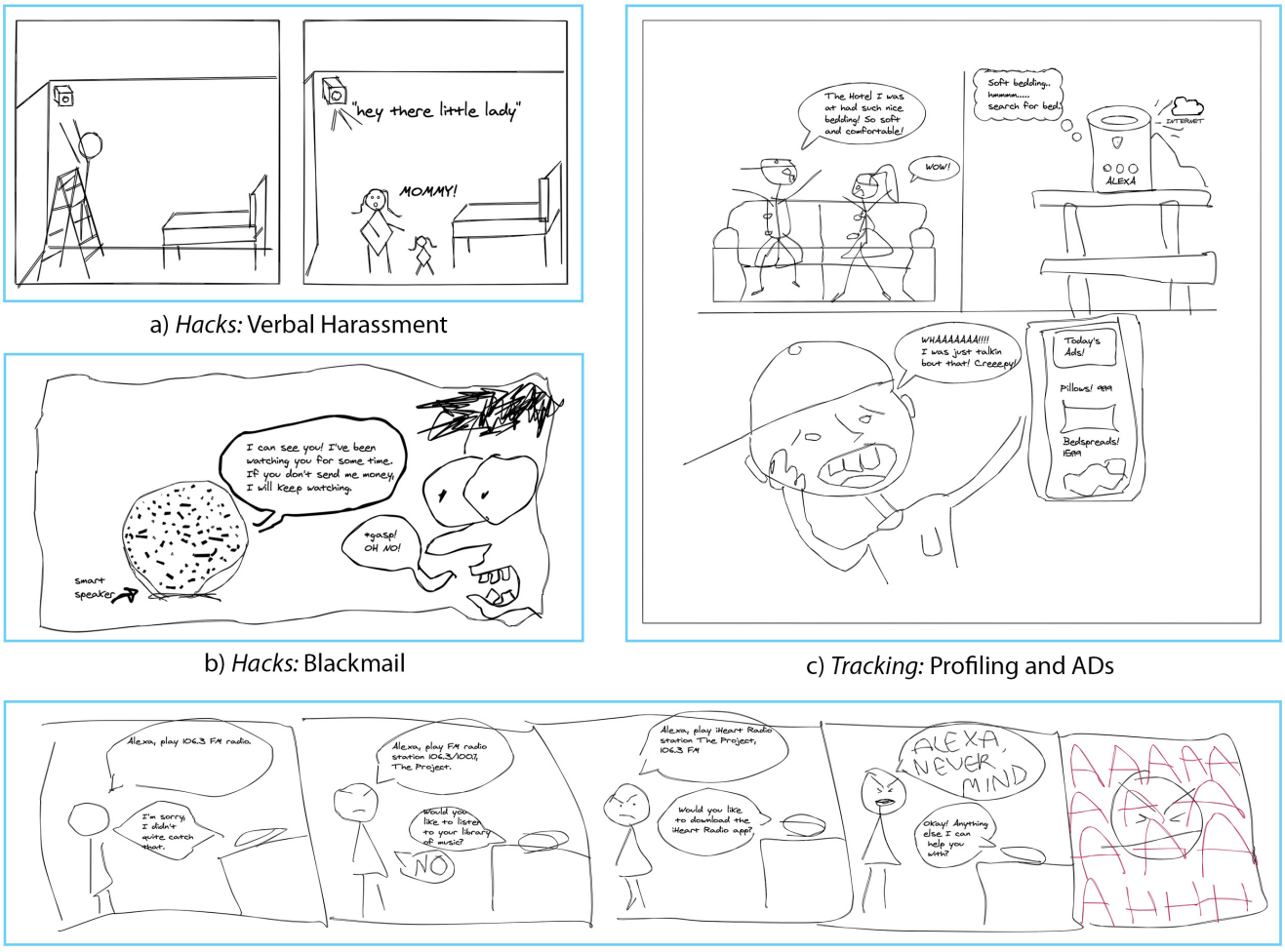


Figure 2: Gallery of negative themes portrayed in the comic narratives.

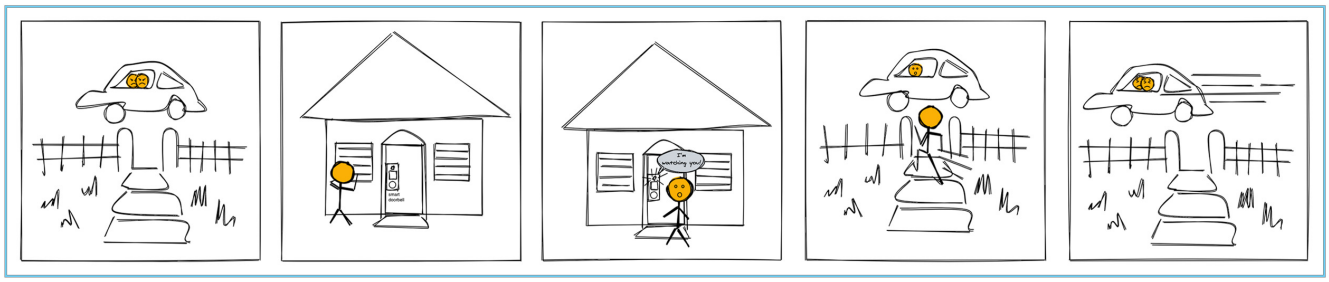
Many stories highlighted the thrill of first encounters with IoT technology, which also amazed the story recipient. For example, P157+ share a story about a friend who was delighted with the ease of controlling the lights and speakers at her house: "[my friend] said she felt like she was living in the future", said P157+.

IoT devices generally enhanced the home experience by automating functions like lighting and music playback. Smart light bulbs that adjust automatically and voice-activated speakers were noted for improving mood and sleep quality. In addition, these devices provided psychological or emotional support, such as playing music or telling jokes at the right moment to uplift spirits.

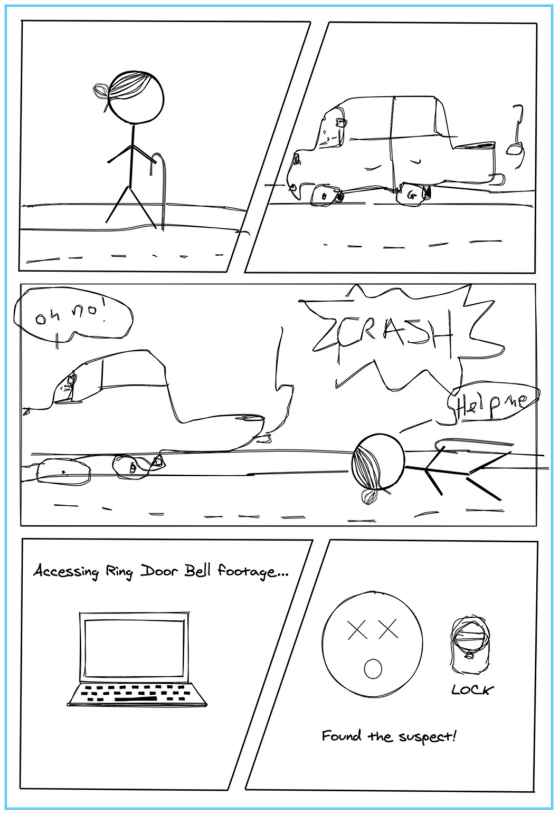
In addition to practical uses, some shared FUNNY MOMENTS captured by IoT devices, such as pets, babies, and wildlife engaging in amusing or mischievous behavior. A few stories also demonstrated how IoT can help CAREGIVING for the elderly, children, and pets. For example, P68+ responded to a story, shown in Figure 3c, of a daughter using devices to check in with her elderly father:

> *I thought this set-up seemed like a great idea for use with an elderly relative, especially when you don't live nearby to always be able to check up on them. I especially liked the 'drop-in' phone call feature, which is quite handy when dealing with someone with early dementia who has trouble learning how to use new devices.*

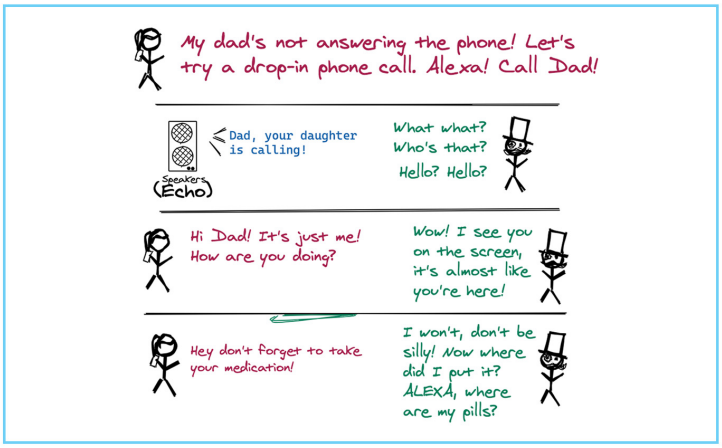
Another participant shared a story about her parents using a smart camera to monitor their Chihuahua while away. After noticing the dog shivering, they used Alexa to turn on a box heater and were relieved to see their dog sitting next to it for warmth. It's such a simple and heartwarming story," said P260+, "but it's really stuck with me as a testament to all the little ways smart devices can improve people's (and animals') lives." Lastly, IoT device were noted for their potential ENERGY SAVINGS capabilities. Figure 3d portrays a story shared by P228+ whose friend's smart thermostat and light systems *"helped him save several thousand dollars over the course of the year."*



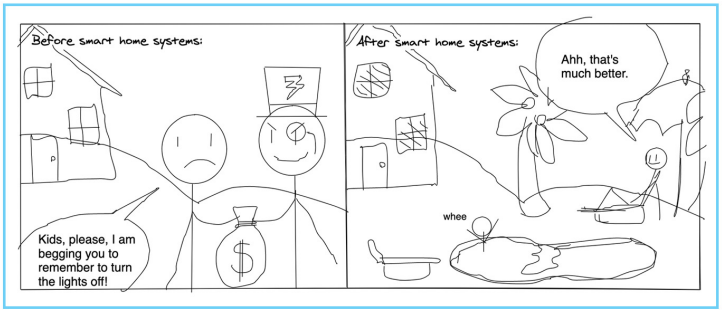
a) *Home Monitoring:* Property Protection



b) *Home Monitoring:* Evidence



c) *Enhance Daily Life:* Caregiving



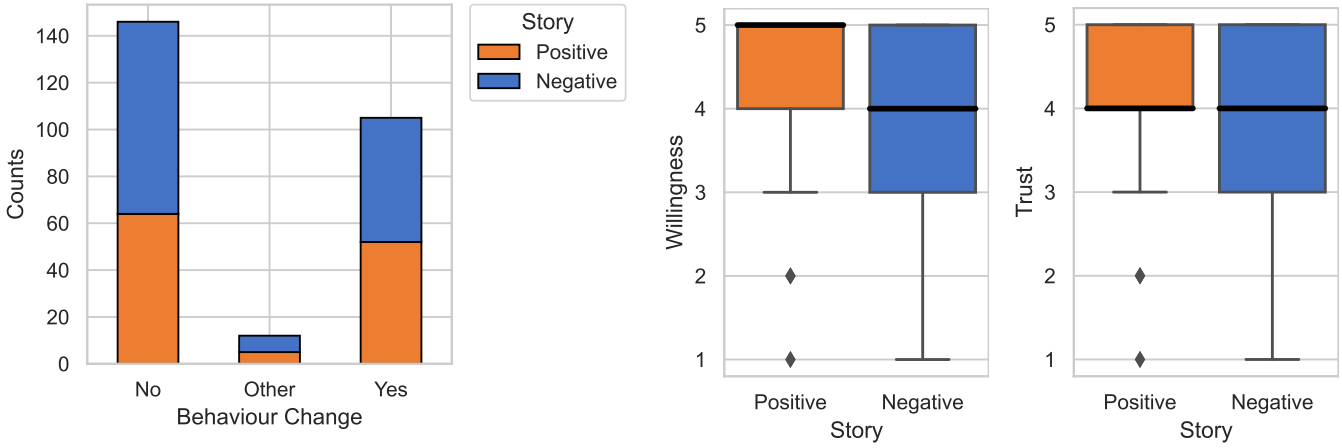
d) *Enhance Daily Life:* Energy Savings

Figure 3: Gallery of positive themes portrayed in the comic narratives.

4.5 Stories' Influence on Perception & Behavior

This section reports the effects of positive and negative IoT stories on participants' self-reported behavior, willingness to use IoT devices, and trust in these devices, as shown in Figure 4. When asked if they had started doing anything differently after hearing a story, 43.3% (n = 114) of participants reported doing so. Figure 4a summarizes the distribution of participants' responses–"yes", "no", or "other"–to whether they changed their behavior after hearing the story. Participants who considered making changes but had not yet committed to them selected the "other" option. No significant differences were observed between participants exposed to positive versus negative stories in terms of overall behavior changes. However, further comparisons of participants' willingness to use and trust in IoT devices (Figures 4b and 4c) revealed statistically significant differences between the two groups. As shown in Table 6, negative stories significantly reduced participants' levels of trust (p = .012) and their willingness to use IoT devices (p < .001) compared to those who heard positive stories.

Among the participants who reported changing their behavior after hearing negative stories (45.8%, n = 65), 27 participants said



(a) Behavior change **(b) Willingness to use IoT devices** **(c) Trust towards IoT devices**

Figure 4: Impact of {positive, negative} stories on behavior and perception changes

that they had disconnected or physically unplugged devices or stopped using them altogether after hearing negative stories.

> *I started to notice that discussions I was having with my husband turned into advertisements.... I had heard from friends that smart devices spy on us...I did an experiment. We took the TV out of the living area and kept it unplugged, Alexa was placed in the garage, our smart security system was unplugged, and we placed our phones outside. I noticed that the advertisements stopped! We have been spied on our entire lives, and smart devices are not a good thing.* (P219^{-})

Another 18 participants reported exercising greater caution around IoT devices, such as being more mindful of their behavior and conversations near IoT devices. 8 participants increased security measures, such as strengthening passwords and adjusting security settings, while another 8 sought alternative IoT manufacturers. Additionally, 4 participants mentioned researching IoT devices online to better understand the associated risks.

Among the participants who reported behavioral changes after hearing positive stories, 89.8% (n = 44), 21 committed to purchasing and installing a new IoT device. 12 participants explored purchasing options by researching online for pricing and availability. 11 participants indicated that they reviewed and updated settings or adopted new features. For example, P104^{+} explained how a story had led to a service upgrade for their smart doorbell.

Table 6: Comparisons of participants' willingness to use and trust after hearing "positive" vs. "negative" stories

	Willingness	median	Mean	SD	Min	Max	Wilcoxon rank-sum test	
Story	**n**							
Positive	121	4	4.041	0.879	1	5	Chi-square	5823.5
Negative	142	4	3.676	1.127	1	5	P	**<.001**
	Trust							
Story	**n**							
Positive	121	5	4.272	0.913	1	5	Chi-square	7114.5
Negative	142	4	3.578	1.24	1	5	P	**0.012**

> *I saw a story about how a doorbell camera can act as a security camera to catch thieves stealing delivery packages from you. There are countless videos online of people caught––and later arrested––for stealing packages thanks to these cameras...After I saw this, I checked my doorbell camera to make sure it was working and then signed up for the yearly monitoring contract, which I had not done when I bought the camera.*

4.6 Factors of Perception and Behavior Change

4.6.1 Behavioral influences. As shown in Table 7, significant predictors of behavior change include `vivid_recall`, `emotions`, `pos_IoT_experience`, and `neg_IoT_experience`. Specifically, participants who recall the story more vividly were significantly more likely to change their behavior (p = .009). Positive emotions such as feeling "excited," (p = .042) or "inspiring" (p = .017), as well as negative emotions like "frustrated" (p = .028), were also linked to a higher likelihood of behavior change. Furthermore, participants who heard negative stories and had previous negative experiences with IoT devices personally were significantly more likely to change their behavior (p = .015) than those who heard negative stories but had no prior negative experiences with IoT devices. However, no significant association was found among those who heard positive stories and had good experiences with IoT devices.

4.6.2 Perception Influences. As demonstrated in Table 8, we identified significant impacts from predictors in participant perceptions toward IoT devices after hearing the story: `vivid_recall`, `seriousness`, `emotions`, and `technical_background`. Participants who recalled the story more vividly reported a significantly higher level of positive effects on their trust in IoT devices (P = .001). Those who heard positive stories and had received formal technical training also expressed significantly higher positive effects on their trust (p = .049). Additionally, participants who felt the positive emotion that the story is "inspiring" reported a significantly higher level of positive effects on their trust (p = .010).

Table 7: Univariate (single-predictor) logistic regression analyses of factors influencing the likelihood of change of behavior. Only predictors with significance ($p < .05$) were included.

Factor	Estimate	Std.Error	z	p	OR (95% CI)
(Intercept)	0.092	0.137	0.676	0.5	1.096 (0.838, 1.435)
vivid_recall	0.046	0.017	2.646	**0.009**	1.047 (1.012, 1.083)

Factor	Estimate	Std.Error	z	p	OR (95% CI)
(Intercept)	0.143	0.188	0.761	0.448	1.154 (0.795, 1.673)
pos_IoT_experience=Yes	0.348	0.193	1.801	0.074	1.416 (0.966, 2.078)

Factors*	Estimate	Std.Error	z	p	OR (95% CI)
(Intercept)	0.343	0.083	4.132	0	1.409 (1.197, 1.659)
emotions=Excited	0.237	0.116	2.047	**0.042**	1.267 (1.009, 1.593)
emotions=Frustrated	0.204	0.092	2.213	**0.028**	1.226 (1.023, 1.47)
emotions=Inspiring	0.233	0.097	2.401	**0.017**	1.262 (1.043, 1.527)

Factor	Estimate	Std.Error	z	p	OR (95% CI)
(Intercept)	0.369	0.046	7.990	0	1.446 (1.32, 1.585)
neg_IoT_experience=Yes	0.244	0.099	2.461	**0.015**	1.276 (1.049, 1.551)

Note. *We performed one-hot encoding on the "emotions" variables. Therefore, each emotion option in the original multiple-choice question becomes a binary variable with "1" representing a participant selected the emotion and "0" representing a participant did not select the emotion. We only included emotions that showed significance ($p < 0.05$) in this table.

Table 8: Univariate (single-predictor) OLS linear regression analyses of factors influencing participants' trust towards IoT devices. Only predictors with significance ($p < .05$) were included.

DV=pos_story_trust_change

Factor	Estimate	Std.Error	z	p	(95% CI)
(Intercept)	2.681	0.400	6.701	<0.001	(1.889, 3.473)
vivd_recall	0.170	0.049	3.465	**0.001**	(0.073, 0.267)

DV=neg_story_trust_change

Factor	Estimate	Std.Error	z	p	(95% CI)
(Intercept)	2.007	0.280	7.175	<0.001	(1.454, 2.560)
seriousness	0.443	0.071	6.255	**<0.001**	(0.303, 0.583)

DV=pos_story_trust_change

Factor*	Estimate	Std.Error	z	p	(95% CI)
(Intercept)	3.872	0.201	19.260	<0.001	(3.473, 4.270)
emotions=Inspiring	0.429	0.164	2.616	**0.010**	(0.104, 0.754)

DV=neg_story_trust_change

Factor*	Estimate	Std.Error	z	p	(95% CI)
(Intercept)	3.01	0.237	12.679	<0.001	(2.540, 3.479)
emotions=Angry	0.415	0.196	2.119	**0.036**	(0.028, 0.803)
emotions=Curious	-0.556	0.194	-2.863	**0.005**	(-0.941, -0.172)
emotions=Distrustful	0.55	0.214	2.566	**0.011**	(0.126, 0.974)

DV=pos_story_trust_change

Factor	Estimate	Std.Error	z	p	(95% CI)
(Intercept)	3.957	0.090	44.161	0.000	(3.780, 4.135)
technical_background=Yes	0.376	0.190	1.981	**0.049**	(0.000, 0.752)

Note. *We performed one-hot encoding on the "emotions" variables. Therefore, each emotion option in the original multiple-choice question becomes a binary variable with "1" representing a participant selected the emotion and "0" representing a participant did not select the emotion. We only included emotions that showed significance ($p < 0.05$) in this table.

Conversely, participants who perceived a higher level of severity from negative stories reported a significantly higher level of negative effects on their trust in IoT devices ($p < .001$). Negative emotions also played a critical role in shaping trust; participants who felt "angry" ($p = .036$) and "distrustful" ($p = .011$) after hearing negative stories reported significantly higher negative effects on their trust, whereas those who felt "curious" expressed a significantly lower level of negative effects ($p = .005$) compared to those who did not experience these emotions.

We identified several predictors regarding participants willingness to use IoT devices after hearing the story. These include `vivid_recall`, `pos_IoT_experience`, `technical_background`, `emotions`, and `seriousness`. As shown in Table 9, participants who recalled the story more vividly expressed a significantly higher level of positive effects on their willingness to use IoT devices ($p = .017$). Those who heard positive stories and had personally experienced positive interactions with IoT devices showed a significantly greater level of positive effects on their willingness to use these devices ($p = .001$) compared to those who only heard positive stories but did not have personal positive experiences. Additionally, participants with a formal technical background who heard positive stories reported significantly higher level of positive effects on their willingness to use IoT devices ($p < .038$).

Participants who felt "excited" ($p = .028$), "inspiring" ($p = .033$), and "thankful" ($p = .015$) after hearing positive stories reported a higher level of positive effects on their willingness to adopt IoT devices compared to those who did not experience these emotions. However, participants who perceived a higher level of seriousness in negative stories showed a significantly higher level of negative effects on their willingness to use IoT devices ($p < .001$). Lastly, those who felt "curious" ($p = .005$) after hearing negative stories showed lower level of negative effects on their willingness to use IoT devices compared to those who did not experience this emotion.

5 DISCUSSION

5.1 Impact of Folk Tales on Technology Perception and Adoption

Our findings indicate that "folk tales"—anecdotal stories heard from others—significantly influence recipients' perceptions and technology practices. We identified key themes in the stories; positive themes focused mainly on the benefits of using IoT devices for home monitoring and improve daily life, while negative themes

Table 9: Univariate (single-predictor) OLS linear regression analyses of factors influencing participants' willingness to use IoT devices. Only predictors with significance ($p < .05$) were included.

DV=pos_story_willingness_change

Factor	Estimate	Std.Error	z	P	(95% CI)
(Intercept)	3.158	0.317	9.958	<0.001	(2.533, 3.782)
vivid_recall	0.096	0.040	2.392	**0.017**	(0.017, 0.175)

DV=pos_story_willingness_change

Factor	Estimate	Std.Error	z	P	(95% CI)
(Intercept)	3.143	0.330	9.534	<0.001	(2.490, 3.796)
pos_IoT_experience=Yes	1.199	0.340	3.531	**0.001**	(0.527, 1.872)

DV=pos_story_willingness_change

Factor	Estimate	Std.Error	z	P	(95% CI)
(Intercept)	4.181	0.093	45.026	<0.002	(3.997, 4.365)
technical_background=Yes	0.412	0.197	2.095	**0.038**	(0.023, 0.801)

DV=pos_story_willingness_change

Factor*	Estimate	Std.Error	z	P	(95% CI)
(Intercept)	3.889	0.212	18.316	<0.001	(3.468, 4.310)
emotions=Excited	0.461	0.206	2.232	**0.028**	(0.052, 0.870)
emotions=Inspiring	0.374	0.173	2.158	**0.033**	(0.031, 0.717)
emotions=Thankful	0.429	0.173	2.476	**0.015**	(0.086, 0.773)

DV=neg_story_willingness_change

Factor	Estimate	Std.Error	z	P	(95% CI)
(Intercept)	1.762	0.309	5.710	<0.001	(1.152, 2.372)
seriousness	0.482	0.078	6.168	**<0.001**	(0.327, 0.636)

DV=neg_story_willingness_change

Factor*	Estimate	Std.Error	z	P	(95% CI)
(Intercept)	3.069	0.270	11.365	<0.001	(2.535, 3.603)
emotions=Curious	-0.632	0.221	-2.856	**0.005**	(-1.069, -0.194)

Note. *We performed one-hot encoding on the "emotions" variables. Therefore, each emotion option in the original multiple-choice question becomes a binary variable with "1" representing a participant selected the emotion and "0" representing a participant did not select the emotion. We only included emotions that showed significance ($p < 0.05$) in this table.

centered around security breaches, surveillance, and device unreliability. In essence, the stories highlighted the risks and benefits of smart home technology. Echoing previous work on users' perceptions [37, 47, 57], security and privacy concerns remain dominant, particularly with regards to voice assistants and smart toys. Negative stories can discourage users from adopting new devices, reduce their usage of existing devices, or diminish trust and willingness to use IoT devices.

We found that previous personal experiences mediate the effects of the stories. Specifically, those who heard negative stories and also had previous negative experiences with IoT devices were more likely to be persuaded compared to those who had not had bad experiences before. This aligns with previous related findings that negative events are more likely to be shared by peers [46] and more likely to encourage adoption of security practices [18]. Previous work also hypothesized that focusing on negative consequences could be more effective in influencing behavior than positive outcomes [18, 41].

However, we found that participants with prior positive experiences exhibited a greater willingness to use IoT devices after hearing positive stories. This suggests that positive stories also play a crucial role in shaping technology adoption, particularly when they emphasize the benefits of technology. Our findings indicate that highlighting the life-enhancing capabilities and safety features can increase users' interest in adopting new devices or expanding their use of existing ones, especially when such stories evoke emotions like excitement and feelings of being inspired.

5.2 Device-Specific Perceptions

We found that user perceptions of different types of IoT devices are shaped based on the nature of stories associated with them. For example, home security systems and utility devices are frequently linked to positive anecdotes that emphasized their role in protecting personal property, improving safety and efficiency, and responding to emergency situations. In contrast, voice assistants, smart toys and baby monitors carried negative connotations, particularity around privacy concerns, unauthorized data collection, and risks to vulnerable members of the household. This suggests that stories about certain types of IoT devices can evoke stronger emotional responses based on their perceived functions and risks. Although this may also be because these devices are framed more positively or negatively on social media, our study highlights that consumers' feelings toward technology, such as anger, distrust, frustration, inspiration, curiosity, and excitement, can significantly influence purchasing decisions and technology adoption.

From a marketing perspective, stories shared among consumers can either elevate or harm the perception of emerging technologies like artificial intelligence (AI), domestic robots, and immersive technologies like virtual reality. Different types of technologies can inspire different types of anecdotal influences. For example, while IoT stories often highlighted tangible harms like stalking or hacking, anecdotal stories about generative AI might center on ethical concerns, misuse, or misinformation. The storytelling approach offers marketers a valuable tool for understanding consumer perceptions and expressions. Our findings reveal that conflicting narratives about particular types of technology often arise. For instance, while some view smart cameras as essential for safety and security, others see them as invasive tools for spying or stalking. Regardless of the origin of these stories, marketers must recognize and address the positive and negative associations surrounding their products. In addition to surveys, stories can be collected from various sources, such as social media, blogs, online forums, user reviews, and social news sites. However, analyzing stories alone may

not fully capture consumer behavior—the emotional and psychological factors within these narratives that drive behavioral patterns should also be considered. By leveraging insights from consumer stories, marketers can refine product messaging to build trust and counter negative perceptions. For example, addressing concerns about spying associated with smart home cameras by emphasizing their role in enhancing home safety.

5.3 Story Authenticity and Validity

Although our study is the first to examine stories in the context of smart home IoT, we believe these narratives are widely shared, especially in personal conversations and on social media. Surprisingly, we found that the types of story source and medium had no significant influence on their trust and willingness to use IoT devices. Whether stories were heard from friends, family, news outlets, or social media, participants reported a similar level of trust toward their authenticity and validity. This suggests that most users trust the stories they encounter, regardless of the credibility of the sources. However, since our findings suggest that stories can significantly shape users' technology perceptions and behavior, this trust also raises concern about the potential for misinformation, where unverified, inaccurate, or exaggerated stories can spread through social media and word of mouth. When misinformation is believed and trusted, particularly about security and privacy risks, it can lead to incorrect mental models, fear, and ineffective practices. Therefore, it is crucial for users to critically assess the stories they hear and for future research to also consider the possibility and impact of misinformation in shaping public perceptions of technology. As a first step, our research cautions that technology design must be aware of popular stories that surface in mass media and word-of-mouth communications, as a way to understand how consumers think about and experience their products to better manage the narrative and meanings of the technology they want to create.

5.4 Lessons Learned From Duo Text and Comic-Based Data Collection

We aimed to explore users perceptions toward IoT devices by collecting their stories in both textual and visual narrative forms, an approach that, to our knowledge, has not been previously employed. Although our primary focus of this work is not to rigorously test this method against traditional single-format elicitation techniques (e.g., sketching [39, 48]), it enabled a glimpse of emerging patterns when utilizing this dual-format approach.

Future research interested in employing the duo-elicitation method should first determine how the combination of textual and visual narrative can help them achieve their research questions and objectives. For the purpose of our study, we coded the visual data for elements that did not exist in the textual version, such as emotional expressions, character dialogues and actions, and narrative structure, which produced a particularly rich dataset that often revealed different aspects of the stories. We suggest that triangulation of textual and visual data enables a more comprehensive understanding of mental models and aspects of user experiences that may not arise in text-only or visual-only formats. For example, our participants often enriched their stories with visual elements and metaphors. One notable form of augmentation was the tendency to exaggerate and more clearly define the story's ending in the comics. In some cases, where the textual endings appeared weak, the comics presented more climatic conclusions. We speculate that this difference arises from the rich visual and expressive notation, such as emojis, grawlix symbols (e.g., $*%&!) and squean symbols (e.g., bubbles, starbursts) available in comics' graphical language, which our participants used to enhance their storytelling.

We found that the visual data helped to better capture the emotional dimensions of users' perception, particularly in amplifying the emotional aspects of the stories. Most comics included multiple panels, with emojis commonly used to convey emotions and amplify the emotional impact. Therefore, we suggest that visual data, such as those portrayed through sketches or comics, can surface deeper emotional responses that may not be fully captured through words alone. It is particularly useful to help participants articulate abstract concepts like privacy and convey complex feelings about their relationships with technology.

Lastly, we argue that the dual-elicitation approach enables participants to express their stories in multifaceted ways. For example, we found that comics often featured more characters than their corresponding textual narratives, indicating that participants added layers of storytelling to enrich their narratives.

5.5 Limitations

There are several limitations to be noted. Our findings reflect the stories and concerns from anecdotal stories collected between March and April 2023. Most of our participants shared stories they had heard within the last three years. As new technologies with advanced data collection capabilities become more prevalent, new privacy concerns and narratives may emerge [13] and require periodic surveys to track the evolving narratives and perceptions of IoT devices and other emerging technologies over time.

Our study aimed to examine the impact of positive and negative stories on people's perceptions and behaviors. However, our findings may not be fully generalizable to the broader population of smart home device users. For example, we recruited participants exclusively through Prolific. While we requested a representative sample, our study does not capture perspectives from smart home users who do not have an account on the platform. To address this limitation, we encourage future research to explore perceptions and attitudes using diverse recruitment channels, such as social media and community forums, which attract different user populations.

To ensure high-quality responses, we implemented fraud detection measures in Qualtrics, included an attention-check question, and incorporated a manual drawing task for additional quality control. However, we acknowledge that fabricated responses cannot be completely eliminated in online studies. Furthermore, while we collected stories from various smart home IoT devices, the majority focused on home security systems and voice assistants, some covering smart home utilities, smart toys, and baby monitors. Due to a limited number of stories, we could not draw conclusions about smart appliances and wearables. We encourage future research to explore these device categories in greater depth.

Our study used an online survey methodology that was well suited for conducting the drawing activity, a critical part of our

study design. While this method provided valuable insights, it limited our ability to ask follow-up questions about the stories. Thus, we encourage future research to further investigate IoT stories with complementary methods, such as interviews and focus groups. These approaches can offer richer insights into how participants interpret and feel about narrative stories.

Lastly, the findings of our study are based on participants' self-reported responses to the stories, which may not always reflect their real behavior. However, since events in the stories we collected are something the participant heard that happened to other people rather than to them personally, we believe it helps to reduce the social stigma of being victim and enabled our participants to share their feelings and reactions more openly to the incidents.

6 CONCLUSION

Our research explored whether stories shared by others that emphasize positive and negative experiences affect the trust and willingness of the story recipients to use IoT devices, even if they have not personally experienced the incidents described in the stories. By analyzing both text and visual narratives from 263 participants in an online survey, we found that stories play a significant role in shaping participants' trust and willingness to adopt these technologies. Negative stories, especially those concerning security, privacy, and device unreliability, were more likely to decrease users' trust and deter device adoption and usage. In contrast, positive stories about the potential for improved safety and quality of life increased interest in using IoT devices. These findings highlight the powerful role of narratives that circulate online and from person to person in shaping technology adoption. IoT designers should consider how narratives, both positive and negative, can affect consumers' acceptance of products and services. We suggest that stories are particularly powerful in strengthening or weakening emotional connections between consumers and technology. Future research can build on these insights by exploring more nuanced perceptions surrounding smart home technologies and specific types of devices, and how crafting narratives might encourage desirable behaviors, such as making informed decisions about security, privacy, and safety, and leading a life enriched by technology rather than hindered by fears of it.

REFERENCES

[1] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J Lee. 2020. Tangible privacy: Towards user-centric sensor designs for bystander privacy. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (2020), 1–28.

[2] Leslie J Albert, Simon Rodan, Nitin Aggarwal, and Timothy R Hill. 2019. Gender and Generational Differences in Consumers' Perceptions of Internet of Things (IoT) Devices. *E-Journal of Social & Behavioural Research in Business* 10, 3 (2019).

[3] Mobark Q Aldossari and Anna Sidorova. 2020. Consumer acceptance of Internet of Things (IoT): Smart home context. *Journal of Computer Information Systems* 60, 6 (2020), 507–517.

[4] Nazanin Andalibi, Oliver L Haimson, Munmun De Choudhury, and Andrea Forte. 2016. Understanding social media disclosures of sexual abuse through the lenses of support seeking and anonymity. In *Proceedings of the 2016 CHI conference on human factors in computing systems*. 3906–3918.

[5] Khadija Baig, Elisa Kazan, Kalpana Hundlani, Sana Maqsood, and Sonia Chiasson. 2021. Replication: Effects of Media on the Mental Models of Technical Users. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS)*. 119–138.

[6] Julia Bernd, Ruba Abu-Salma, Junghyun Choy, and Alisa Frik. 2022. Balancing power dynamics in smart homes: Nannies' perspectives on how cameras reflect and affect relationships. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 687–706.

[7] Flora Bowden, Dan Lockton, Rama Gheerawo, and Clare Brass. 2015. Drawing energy: Exploring perceptions of the invisible. (2015).

[8] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. 2016. On privacy and security challenges in smart connected homes. In *2016 European Intelligence and Security Informatics Conference (EISIC)*. IEEE, 172–175.

[9] Shi-Yi Chen, Zhe Feng, and Xiaolian Yi. 2017. A general introduction to adjustment for multiple comparisons. *Journal of thoracic disease* 9, 6 (2017), 1725.

[10] Victoria Clarke, Virginia Braun, and Nikki Hayfield. 2015. Qualitative psychology: A practical guide to research methods. *Qualitative Psychology* (2015), 222–248.

[11] Andrew Cox and Melanie Benson. 2017. Visual methods and quality in information behaviour research: The cases of photovoice and mental mapping. *Information Research: An International Electronic Journal* 22, 2 (2017), n2.

[12] Cassandra Cross, Megan Parker, and Daniel Sansom. 2019. Media discourses surrounding 'non-ideal'victims: The case of the Ashley Madison data breach. *International Review of Victimology* 25, 1 (2019), 53–69.

[13] Ben Egliston and Marcus Carter. 2023. Examining visions of surveillance in Oculus' data and privacy policies, 2014–2020. *Media International Australia* 188, 1 (2023), 52–66.

[14] Pardis Emami Naeini, Martin Degeling, Lujo Bauer, Richard Chow, Lorrie Faith Cranor, Mohammad Reza Haghighat, and Heather Patterson. 2018. The influence of friends and experts on privacy decision making in IoT scenarios. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–26.

[15] Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor. 2021. Which privacy and security attributes most impact consumers' risk perception and willingness to purchase IoT devices?. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 519–536.

[16] Motahhare Eslami, Karrie Karahalios, Christian Sandvig, Kristen Vaccaro, Aimee Rickman, Kevin Hamilton, and Alex Kirlik. 2016. First I" like" it, then I hide it: Folk Theories of Social Feeds. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 2371–2382.

[17] Matthias Fassl, Alexander Ponticello, Adrian Dabrowski, and Katharina Krombholz. 2023. Investigating Security Folklore: A Case Study on the Tor over VPN Phenomenon. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW2 (2023), 1–26.

[18] Chris Fennell and Rick Wash. 2019. Do stories help people adopt two-factor authentication. *Studies* 1, 2 (2019), 3.

[19] Andy Field, Zoe Field, and Jeremy Miles. 2012. *Discovering statistics using R*. sage.

[20] Batya Friedman, David Hurley, Daniel C Howe, Helen Nissenbaum, and Edward Felten. 2002. Users' conceptions of risks and harms on the web: A comparative study. In *CHI Extended Abstracts in Conference on Human Factors in Computing Systems*. 614–615. https://doi.org/10.1145/506443.506510

[21] Kelsey R Fulton, Rebecca Gelles, Alexandra McKay, Yasmin Abdi, Richard Roberts, and Michelle L Mazurek. 2019. The Effect of Entertainment Media on Mental Models of Computer Security. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS)*. 79–95.

[22] Susan A Gelman and Cristine H Legare. 2011. Concepts and Folk Theories. *Annual Review of Anthropology* 40 (2011), 379–398.

[23] Abir Ghorayeb, Rob Comber, and Rachael Gooberman-Hill. 2021. Older adults' perspectives of smart home technology: Are we developing the technology that older people want? *International journal of human-computer studies* 147 (2021), 102571.

[24] Markus Giesler and Eileen Fischer. 2018. Iot stories: The good, the bad and the freaky. *NIM Marketing Intelligence Review* 10, 2 (2018), 24–28.

[25] Damian Gordon. 2010. Forty Years of Movie Hacking: Considering the Potential Implications of the Popular Media Representation of Computer Hackers From 1968 to 2008. *International Journal of Internet Technology and Secured Transactions* 2, 1-2 (2010), 59–87.

[26] 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*. 1–25.

[27] Beth L Hoffman, Ariel Shensa, Charles Wessel, Robert Hoffman, and Brian A Primack. 2017. Exposure to fictional medical television and health: a systematic review. *Health education research* 32, 2 (2017), 107–123.

[28] Timo Jakobi, Sameer Patil, Dave Randall, Gunnar Stevens, and Volker Wulf. 2019. It is about what they could do with the data: A user perspective on privacy in smart metering. *ACM Transactions on Computer-Human Interaction (TOCHI)* 26, 1 (2019), 1–44.

[29] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "my data just goes everywhere:" User mental models of the internet and implications for privacy and security. In *Symposium On Usable Privacy and Security*. 39–52. https://dl.acm.org/doi/10.5555/3235866.3235870

[30] Patrice A Keats. 2009. Multiple text analysis in narrative research: Visual, written, and spoken stories of experience. *Qualitative Research* 9, 2 (2009), 181–195.

[31] Willett Kempton. 1986. Two Theories of Home Heat Control. *Cognitive science* 10, 1 (1986), 75–90.

[32] Klaus Krippendorff. 2004. Reliability in content analysis. *Human communication research* 30, 3 (2004), 411–433.
[33] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–31.
[34] David Lee. 2018. *Amazon promises fix for creepy Alexa laugh.* Retrieved July 2023 from https://www.bbc.com/news/technology-43325230
[35] Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. 2017. Toys that listen: A study of parents, children, and internet-connected toys. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 5197–5207.
[36] Sarah Mennicken and Elaine M Huang. 2012. Hacking the natural habitat: an in-the-wild study of smart homes, their development, and the people who live in them. In *Pervasive Computing: 10th International Conference (Pervasive 2012)*. Springer, 143–160.
[37] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy expectations and preferences in an {IoT} world. In *Thirteenth symposium on usable privacy and security (SOUPS 2017)*. 399–412.
[38] Don Norman. 2013. *The design of everyday things: Revised and expanded edition.* Basic books.
[39] Maggie Oates, Yama Ahmadullah, Abigail Marsh, Chelse Swoopes, Shikun Zhang, Rebecca Balebako, and Lorrie Faith Cranor. 2018. Turtles, locks, and bathrooms: Understanding mental models of privacy through illustration. *Proceedings on Privacy Enhancing Technologies* 2018, 4 (2018), 5–32. https://doi.org/10.1515/popets-2018-0029
[40] Sunyup Park, Anna Lenhart, Michael Zimmer, and Jessica Vitak. 2023. "Nobody's Happy": Design Insights from {Privacy-Conscious} Smart Home Power Users on Enhancing Data Transparency, Visibility, and Control. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS)*.
[41] Katharina Pfeffer, Alexandra Mai, Edgar Weippl, Emilee Rader, and Katharina Krombholz. 2022. Replication: Stories as Informal Lessons about Security. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 1–18.
[42] Erika Shehan Poole, Marshini Chetty, Rebecca E Grinter, and W Keith Edwards. 2008. More than meets the eye: transforming the user experience of home network management. In *Proceedings of the ACM Conference on Designing Interactive Systems*. 455–464.
[43] Emilee Rader and Rebecca Gray. 2015. Understanding user beliefs about algorithmic curation in the Facebook news feed. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. 173–182.
[44] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*. 1–17.
[45] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J Aviv. 2019. "Woe is me:" Examining Older Adults' Perceptions of Privacy. In *CHI Extended Abstracts in Conference on Human Factors in Computing Systems*. 1–6. https://doi.org/10.1145/3290607.3312770
[46] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. 2016. I think they're trying to tell me something: Advice sources and selection for digital security. In *IEEE Symposium on Security and Privacy (SP)*. IEEE, 272–288.
[47] Asreen Rostami, Minna Vigren, Shahid Raza, and Barry Brown. 2022. Being Hacked: Understanding Victims' Experiences of {IoT} Hacking. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 613–631.
[48] Miriam Sturdee, Lauren Thornton, Bhagya Wimalasiri, and Sameer Patil. 2021. A Visual Exploration of Cybersecurity Concepts. In *Creativity and Cognition*. 1–10.
[49] Sangho Suh, Sydney Lamorea, Edith Law, and Leah Zhang-Kennedy. 2022. PrivacyToon: Concept-driven Storytelling with Creativity Support for Privacy Concepts. In *Proceedings of the 2022 ACM Designing Interactive Systems Conference* (Virtual Event, Australia) *(DIS '22)*. Association for Computing Machinery, New York, NY, USA, 41–57. https://doi.org/10.1145/3532106.3533557
[50] Parth Kirankumar Thakkar, Shijing He, Shiyu Xu, Danny Yuxing Huang, and Yaxing Yao. 2022. "It would probably turn into a social faux-pas": Users' and Bystanders' Preferences of Privacy Awareness Mechanisms in Smart Homes. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–13.
[51] Joseph Turow. 2010. *Playing doctor: Television, storytelling, and medical power.* University of Michigan Press.
[52] United States Census Bureau. 2022. *ACS Demographic and Housing Estimates.* Retrieved Apr 2024 from https://data.census.gov/table/ACSDP5Y2022.DP05?q=DP05&y=2022
[53] Rick Wash. 2010. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*. 1–16.
[54] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300428
[55] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy perceptions and designs of bystanders in smart homes. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–24.
[56] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security & privacy concerns with smart homes. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security* (Santa Clara, CA, USA) *(SOUPS '17)*. USENIX Association, USA, 65–80.
[57] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–20.

A QUESTIONNAIRE

A.1 Instructions

We are interested in (positive or negative) stories related to Internet of Things (IoT) devices in smart homes that you have read or heard about—that is, stories about OTHER PEOPLE's experiences—from a friend, coworker or acquaintance, social media sites, blogs, newspapers, or any other source you can think of.

Positive stories about home IoT devices might include things like: enhanced safety and security (e.g., catching break-ins, monitoring safety), increased productivity, efficiency, and accessibility of the home, or other stories that had significantly influenced your POSITIVE perception and interaction towards IoT devices in the home setting.

Negative stories about home IoT devices might include things like: hacks, devices "acting up", rogue recordings, invasion of personal privacy or privacy of others, attackers hijacking and controlling a device, data and identity theft, spying and surveillance, unauthorized location tracking, data manipulation, and misuse of shared IoT devices in a household, or other stories that had significantly influenced your NEGATIVE perception and interaction towards IoT devices in the home setting.

A.2 Story characteristics

We will start with three open-ended questions to help you remember stories you may have heard or read about IoT devices in home settings. Afterwards, we will continue with multiple choice questions.

1. Take a moment to think back to times in the past when you remember being told or reading about a story related to IoT devices in the home. Please make a list of *as many* of these stories *as you can remember*, using only a couple of words to describe each story. *[Textboxes] (Enter one story per line)*
2. Finally, please choose ONE story for which you can most easily recall details about where you were and what happened when you heard or read about it. *[Textbox] In a sentence or two, briefly summarize what happened.*
3. On a scale of 1–10, how vividly do you recall the details of the story? *[5-point scale] (1 = Least vivid; 10 = Most vivid)*
4. How long ago did you hear or read the story? *Within the last day Within the last day, Within the last week, Within the last month, Within the last year,Within the last three years, Longer than three years ago, Don't remember*
5. Via what medium did you hear or read the story? *[Textbox] In person (face-to-face), Phone, Text message, Chat (instant messaging), Video chat, Email, Blog post, Social network site (TikTok, Facebook, Twitter, Instagram, LinkedIn etc.), Print news media (physical newspaper, magazine, etc.), Broadcast news media (TV,*

Radio, etc.), Online news media (CNN.com, Yahoo News, etc.), Don't remember, Other (please specify)

6. From what source did you hear or read the story? *Family member, Friend, Acquaintance, Coworker or Boss, IT or Computer Repair Person, Stranger, News Institution, Don't Remember, Other (please specify)*
7. Is your story a positive or negative one? *(Positive story that had a positive influence on my perception/attitude towards IoT devices in the home settings. Negative story that had a negative influence on my perception/attitude towards IoT devices in the home settings.)*

A.3 Beliefs and Behavior

8. Did you start doing anything differently after hearing this story?*(Yes, No, Other (Please specify) [Textbox])*
9. What did you do differently? *[Textbox]*
10. Do you believe this story actually happened? *(Yes, No, I am not sure)*
11. How serious was the threat or problem? *[5-point scale] (1 = Not at all serious, 5 = Extremely serious)*
12. How much does the story bring to mind the following emotions when you think about the IoT device in the story? *[Multiple choice] ([Negative emotions]: Sad, Helpless, Curious, Angry, Anxiousness, Distrustful, Frustrated, Other [Textbox]; [Positive emotions]: Happy, Excited, Thankful, Proud, Calm, Inspiring, Amused, Other [Textbox])*
13. How much do you think hearing this story has
    a. positively affected your trust towards IoT devices? *[5-point Scale] (1 = Not at all to 5 = A lot) Note: Conditional question shown only to participants who selected positive stories in Q7.*
    b. negatively affected your trust towards IoT devices? *[5-point Scale] (1 = Not at all to 5 = A lot) Note: Conditional question shown only to participants who selected negative stories in Q7.*
14. How much do you think hearing this story has
    a. positively affected your willingness to use IoT devices? *[5-point Scale] (1 = Not at all, 5 = A lot) Note: Conditional question shown only to participants who selected positive stories in Q7.*
    b. negatively affected your willingness to use IoT devices? *[5-point Scale] (1 = Not at all, 5 = A lot) Note: Conditional question shown only to participants who selected negative stories in Q7.*
15. What are IoT devices? [Attention check question] *[Multiple choice] (IoT devices are stand alone devices which are consisting of different types of hardware such as sensors and computational software that do not share information with other devices and systems over the internet, IOT devices are network connected devices which are consisting of different types of hardware such as sensors and computational software sharing information with other devices and systems over the internet)*

A.4 Retelling story

16. First, for the story you recalled in the previous questions, please describe the story as if you were to tell, send, post, or otherwise share this story with somebody else. *[Textbox] For example, to a friend, a family member, a coworker, or an acquaintance. Use as much detail as you can, including any thoughts or recollections you might have had about what happened. Use at least 4-5 sentences to describe the story.*
17. Can you briefly describe the narrative of the comic you created? *[Textbox] We are asking to make sure we are interpreting your comic correctly.*
18. Would you send, post or share your comic with anybody else? *[Multiple choice] (Yes, No, It depends)*
19. Please elaborate on your response above. *[Textbox] (For example, Why did you choose the respective option?)*
20. With whom might you share the comic with? *[Multiple choice] (a friend, a family member, a coworker, or an acquaintance, IT or Computer repair person, Stranger, News institution, Other [Textbox])*
    1. Please explain why *[Textbox] (i.e., why you want to share with that particular group(s)?)*
21. Via what medium would you share the story? *[Multiple choice] (In person (face-to-face), Phone, Text message, Chat (instant messaging), Video chat, Email, Blog post, Social network site (Instagram, Facebook, Twitter, etc.), Other [Textbox]*
22. Do you have any feedback about how we might improve the drawing tool? *[Textbox]*

A.5 Demographic Questions

23. Which, if any, of the following types of Internet-connected device(s) do you own in your household? *[Multiple choice] (Smart appliances (e.g., gas/electric meters, refrigerators, thermostats, or robotic floor cleaners), Smart media devices (e.g., printers, speakers, TVs), Wearables (e.g., smart watches, augmented reality (AR) glasses), Medical health monitors (e.g., Smart continuous glucose monitoring (CGM) and insulin pens, smart inhalers, smart heart monitors), Home assistants (e.g., Amazon Alexa or Google Assistant), Home security systems connected to the Internet (e.g., SimpliSafe), Toys, baby monitors, or GPS child trackers connected to the Internet (e.g., Hello Barbie, Furby Connect, Philips Avent, Amber Alert), Smart light switches, Other [Textbox], I don't own an IoT device)*
24. Have you personally had negative experiences with IoT devices? *(Yes, No)*
25. Which gender do you identify as? *(Female, Male, Non-binary, Prefer to self-describe, Prefer not to answer)*
26. What age group do you belong to? *(19 years and under, 20–24 years, 25–29 years, 30–34 years, 35–39 years, 40–44 years, 45–49 years, 50–54 years, 55–59 years, 60–64 years, 65–69 years, 70–74 years, 75–79 years, 80+ years, Prefer not to answer)*
27. What is your highest level of education? *If you are currently in school, please choose the degree that you are enrolled in. (Less than a high school degree, High school degree or equivalent, College degree, Bachelor's degree, Master's degree, Doctoral degree, Other professional degree, Prefer not to answer)*
28. Please specify your prior experience with digital drawing tools? *(i.e., Adobe, Canva, Paint, etc.) (No experience, Some experience, Much experience)*
29. Please specify your prior experience with drawing comics. *(No experience, Some experience, Much experience)*
30. How frequently do you draw? *(Never, Once every few years, Once a year, Once in several months, Once a month, Once a week)*
31. Have you ever received formal training in computer science, software engineering, IT, computer networks, or a related technical field? *(Yes, No)*