User's perceptions and tolerance of risk and their self-reported concerns of consumer products with internet connectivity

Sarah C Jenkins[1] and Magda Osman[1,2]

1. Department for Analytics, Technology and Operations, Centre for Decision Research, Leeds University Business School, Maurice Keyworth Building, University of Leeds, Leeds, LS2 9JT, UK

2. Judge Business School, University of Cambridge, Trumpington St, Cambridge CB2 1AG, UK.

Correspondence: S.C.Jenkins@leeds.ac.uk

Data availability: All materials and raw data are available at: https://osf.io/cguj4/files

Funding: This report is independent research, with data collection funded by the Office for Product Safety and Standards (OPSS) within the Department for Business and Trade (UK). The opinions and conclusions articulated here are those of the authors and do not represent those of the Office for Product Safety and Standards nor the Department for Business and Trade.

Acknowledgments: This work would not have been possible without the assistance of Binju.

Declarations of interest: The authors declare no competing interests.

Abstract

The steady rise of consumer products with internet connectivity (e.g. voice assistants, smart door locks, smart speakers) (CPIC) in people's homes means that users face a complex array of potential hazards and harms. A pilot study ran in 2023 using a mixed methods design sought to increase the evidence base regarding CPIC with the practical aim that it could inform risk management decisions. A nationally representative sample of 854 UK participants provided ratings concerning their perceptions of risks concerning 10 CPIC (smart: watch, pet feeder, speaker, doorbell, toothbrush, door lock, robot sweeper, teddy camera, connected children's toy and bluetooth tracker). A two-component solution (consisting of concern and benefits) was found to explain 89.3% of the variation in risk perceptions. Attitudes towards new technology were key in predicting levels of risk tolerance. In terms of specific risks participants were concerned by, data security concerns were most frequently rated the highest, with concerns about physical health and social relationships lowest. Data leakage (inadequate warnings or instructions) was deemed the most common cause of risks associated with CPIC. Over 5000 separate free text concerns for CPIC were analysed in response to the open question "What is the biggest risk you could envision associated with this product?". Similar to the quantitative ratings, the most common concerns were around risks to do with data handling (privacy, storage, collection) and criminal activity from unauthorised internet access via the devices. Concerns of risks of a psychological nature made up only 5% of the overall reports. Our findings indicate that normal product functioning does not necessarily allay public concerns when it comes to CPIC, with results highlighting several areas of consumer concerns (data issues, criminal usage) that would be fruitful for regulators to focus their efforts towards.

Keywords: Smart products; connectable consumer products, internet of things; psychological harm; digital risks

In the last decade, technological growth and development has occurred exponentially and as such, consumers have never experienced such convenience, with experts arguing we are now in a new digital age. The ownership of consumer products with internet connectivity (CPIC) (also referred to as 'smart devices', 'smart homes' or 'internet of things' (Briggs et al., 2025; Li et al., 2025; Seymour et al., 2024) has increased rapidly in the past 10 years and is only set to grow further. Eighty percent of consumers own at least one smart home product, with the number of households owning three or more products doubling to 38% since 2019 (GfK, 2024). Across various consumer surveys, the three most popular smart products are consistently smart televisions, smart speakers and smart fitness trackers (GfK, 2024; Ipsos MORI, 2020; Statista, 2025).

Because the nature of CPIC is such that they connect to other devices via a wireless sensor network, how they can go wrong cascades through more than one product, and what solutions are appropriate get obscured. Even if CPIC function as normal or intended, they can still be unpredictable and unreliable (He et al., 2019; Oliveira et al., 2020; Shank et al., 2021), which also presents has implications for how to risk manage these types of products. Understandably then, empirical work has been exploring the mapping between the technological, safety and security issues associated with CPIC. As neatly reviewed by Osman (2025b), technological issues relate to energy efficiency, cost and data quality. Security breaches are the most common hazard associated with CPIC, and spill over into safety issues where unconsented access to data and associated privacy intrusions, extend to criminal activities potentially leading to property damage, financial losses and physical harm.

Through exposure of these types of issues, practical responses in the world of policy making and regulation is to explore new approaches to risk analysis such as how to estimate public exposure of novel hazards (e.g. security vulnerabilities) and novel harms (e.g. non-

physical harm) from CPIC (for examples see Osman, 2025b) in risk assessments. Whilst traditionally, physical harm has been the predominant focus of risk assessments, more recently, attention has turned to whether psychological harm (for review see Osman, 2025a). However, within the realm of CPIC there are concerns it may not meaningfully exist as a discrete concept, or even be possible to measure (e.g. Heath, 2025; Jenkins & Ayton, 2025; Osman, 2025a, 2025b; Zeelenberg & Kogler, 2025). What is meant by psychological harm is that there are aspects of the functioning of smart products that create undue mental or emotion detriments to a level that would impair users' life and wellbeing from baseline and for a considerable period (e.g. Heath, 2025). Whilst psychological harm and associates (e.g. mental harm, emotional distress, psychological damage) are all theoretically possible, very little is known about the frequency of how much these occur in reality, nor the day to day experiences of consumers (though for an exception, see (Cohen et al., 2023; Hunte et al., 2024; Zhu et al., 2021). Therefore, understanding user's concerns and perceptions of CPIC from the view of novel harms, such as psychological harms would go some way to informing how policy makers and regulators approach it when it comes to risk assessing exposure.

Along with risk assessment, the complement to it that policy makers and regulators are also considering is risk management, and within that is an appreciation of public perceptions and tolerances of risks, especially novel ones. That is, the uptake of risk management measures depends in part on their acceptability in the public domain, and that is largely reflective of how the public perceive (e.g. Renn, 1998) and tolerate the risks (e.g. Bouder et al., 2007). Crucially for policy makers and regulators, it is these risk perceptions which feed into a consumer's *risk tolerance*, which has direct implications for consumer behaviour. Risk tolerance refers to the intuitive calculation people make where they evaluate the overall risks against the benefits of a situation, product, or service (Jenkins et al., 2024).

The trade-off of overall risks against benefits reveals that general tolerance of risk, where high tolerance indicates the benefits outweigh the risks and a low tolerance indicates the risks outweigh the overall benefits. Whilst it is logical that one must perceive a risk in order take action in response to it (as evidenced across a variety of contexts), risk perceptions are not always a consistent predictor of behaviour (Anderson et al., 2024; Wachinger et al., 2013). What also matters is an individual's risk tolerance – the extent to which they trade off this perceived risk versus benefits (Jenkins et al., 2024; Office for Product Safety & Standards, 2024). Benefits have consistently been demonstrated to be inversely related to risks perceived (Alhakami & Slovic, 1994; Finucane et al., 2000; Jenkins et al., 2022), and risks tolerated, if the benefit is believed to outweigh the risk (Jenkins et al., 2024). Moreover, given the known risk paradox, which suggests that risk perceptions fail to reliably predict behaviour, risk tolerance has been shown to be a better indicator of actual behaviour (e.g. Jenkins et al., 2024)[1].

Given the paucity of work in the domain of public perceptions of risks attributed to consumer products, it is not clear whether the findings discussed here would similarly apply to CPIC. There are lots of reasons why risk perceptions and tolerance, and indeed the drivers of these, could conceivably differ for CPIC versus their non-connected counterparts. Most

[1] Knowledge concerning how individuals perceive risks of consumer products is relatively limited, with much research dating back to the 1980s (Vaubel & Young, 1992a; Wogalter et al., 1986, 1987; Young et al., 1992; Young & Laughery, 1994). This used the psychometric paradigm and found that risk perceptions are typically underpinned by two or three component solutions. More recently, this psychometric approach was refreshed to measure perceptions of over 100 products (general and personal cosmetics) (Jenkins et al., 2024; Office for Product Safety & Standards, 2024), and extended to incorporate interactive effects between factors. This research found that risk perceptions were found to be driven by a combination of: three *cognitive dimensions* (benefits, dread and individual responsibility), *product category* (i.e. whether a product was a household or leisure product, used more so by vulnerable groups) and *individual differences* (age, gender, being a parent and cultural worldview).

notably, the perceived level of benefits and convenience offered by CPIC, which are a key motivator in intentions to adopt such technology (Li et al., 2021); though high perceived benefits are typically associated with lower risk perceptions (Alhakami & Slovic, 1994; Jenkins et al., 2021, 2024). In addition, relative levels of (un)familiarity (Vaubel & Young, 1992b), ambiguity over levels of individual responsibility for harm, their abstract nature (Jenkins & Ayton, 2025) as well as individual differences in technological literacy/nativeness (Briggs et al., 2025; Klobas et al., 2019; Nicholson et al., 2025) can impact how risk associated with such products is perceived, though there is little to show how the risks are tolerated (e.g., Hunte et al., 2024). Such characteristics mean it is even more important to understand precisely how consumers perceive and tolerate risks associated with CPIC, rather than assuming previous research can be extrapolated to this context.

The timing of the present study is particularly pertinent given the changing regulatory context, with countries across the globe starting to consider the risks posed by CPIC by way of legislation (for examples see Osman, 2025b). In April 2024, in the UK, the Product Security and Telecommunications Infrastructure (PTSI) (Product Security) legislation came into effect, requiring manufacturers to comply with baseline security requirements. The Office for Product Safety and Standards (OPSS), the UK's national regulator for product safety and standards) is responsible for its enforcement on behalf of the Department for Science, Innovation and Technology. This is but one example; given the complexities of such products, it is little wonder that regulatory divergences exist between different countries. Part of this stems from differences in the way harm is conceptualised – viewed either at an individual level, in relation to specific activities or instances causing harm (whether physical or psychological) versus harm to both individuals on a societal level (Farrand, 2024). Although this nuance has important implications for the regulatory direction of travel, very little

research has been dedicated to understanding it. Therefore, there is a need to deepen our understanding of how consumers think about the risks associated with CPIC to inform risk management and communication efforts – essentially to know what is being legislated against. We argue that legislative efforts will be most effective when they are evidence based and aligned with consumer perceptions. The current study therefore aimed to bridge this gap, asking:

1. How are risks associated with CPIC perceived?
2. What personal characteristics predict risk perceptions of CPIC?
3. Do individuals distinguish between different types of risks associated with CPIC?
4. Do individuals distinguish between different causes of risks associated with CPIC?
5. What kinds of concerns do people volunteer when thinking about CPIC?

Methods

Participants

A sample of 854 participants was recruited from the online participant platform Prolific Academic (www.prolific.ac). Participants were required to be over 18 (in order to meet ethical requirements), to have an approval rate of 95-100% and to be located in the UK. Participants were paid £1.70 for the study. Participants were excluded for completing the study unreasonably quickly (<5 minutes), had not fully completed the study, or if their responses for any of the ratings of products had a SD < 0.5, leaving a final sample of 791, for characteristics see Table 1. On average participant took *M* = 17.06 minutes (SD = 19.26 minutes) to complete the study. Informed consent was obtained from all participants. Ethical approval was granted from the University of XXXXX Research Ethics Committee (AREA 17-055). All methods were carried out in accordance with relevant guidelines and regulations.

Table 1. Characteristics of Final Sample

Demographic	Category	n (Percentage)
	Total sample post exclusions (n)	791
Gender	Male	389 (49.2)
	Female	398 (50.3)
	Not specified, stated	3 (0.38)
	Prefer not to say	1 (0.13)
Age	18 - 24	66 (8.3)
	25 - 34	207 (26.2)
	35 - 44	234 (29.6)
	45 - 54	139 (17.6)
	55 - 64	91 (11.5)
	65+	54 (6.8)
	Prefer not to say	0
Children under the age of 18	None	498 (63.0)
	Prefer not to say	4 (0.5)
	Yes, aged between 0-10	2 (0.3)
	Yes, aged between 11-18	58 (7.3)
	Yes, aged between 0-10 and 11-18	71 (9.0)

Overall, scores on the trust/pursuit of new technology measure were just over the midpoint (M= 4.63, SD= 1.29), as were ratings of the importance of internet connectable consumer products to one's daily life (M= 4.51, SD= 1.70). For full breakdown, see Supplementary Materials 1.

Stimuli

The study included ten smart products that were available on the market including their prevalence and topicality (Statista, 2025): (smart pet feeder, smart speaker, teddy camera, connected children's toy, smart doorbell, smart toothbrush, bluetooth tracker, smart door lock, smart robot sweeper and smart watch). Each product was presented with a short descriptive sentence to provide context, though no mention of associated risks or benefits

was made. For the full list of products and their associated descriptions, see Supplementary Materials 2.

Procedure

The study was run using the Qualtrics online survey platform (www.qualtrics.com). Before beginning the main study, participants were asked a series of demographic questions. They were asked to indicate: gender (male/female/other – please specify/prefer not to say); age; if they had children under the age of 18 (Yes – aged between 0-10/Yes – aged between 11-18/Both/No/Prefer not to say) and two questions on attitudes towards new technology and CPIC. Attitudes to new technology was operationalised as "How much do you trust or seek out new technologies/innovations in your daily life? rated from 1 (*Do not trust/seek out at all*) to 7 (*Completely trust/seek out a lot*). Importance of CPIC was operationalised as: "How important are internet connectable consumer products to your daily life? rated from 1 (*Not at all important*) to 7 (*Extremely important*). They were also asked for their Prolific ID, used for payment.

Table 2. Main questions posed to participants regarding risk perceptions for quantitative analysis

Product Characteristics

Product Characteristics
All questions were presented with a Likert scale from 1 to 7 and the text in parentheses represents the anchor points of the Likert Scale
Familiar How familiar are you with the above product? *(Not at all familiar to Extremely familiar)*
Frequency If you own (or were to own) the above product, how often would you use it? *(Never to Daily)*
Benefit Estimate what you think the level of benefit is associated with the above product to you personally? *(No benefit at all, Very great benefit)*
Worry How worried are you about the potential risks associated with the use of this product? *(Not worried at all, Extremely worried)*
Control If exposed to the product, to what extent can you, by personal skill, diligence or training, avoid the hazards associated with the above product? That is, how much control do you have over being harmed by the product? *(No control at all, Total)*
Knowledge of Risk To what extent are the risks associated with this product known precisely to the persons who are exposed to the risk? (*Completely unknown to Known Precisely)*
Concern about Data Usage When using this product, how much are you concerned by how the product stores and uses your personal data for its personalized operation? *(Not at all concerned to Extremely concerned)*
Vulnerable Groups Interaction To what extent do you agree that vulnerable groups (such as children or the elderly) use or interact with the above product more than other groups of people? *(Completely disagree to Completely agree)*
Consider Risk when Purchasing If you were to purchase/have purchased this product, how much would/did you consider the potential risks associated with its use? *(Would not consider at all to Would consider a lot)*
Biggest Risk What is the biggest risk you could envision associated with this product? Please write 1-2 sentences. (For example: Smartphones eavesdrop on people's conversations, smart washing machines analyse laundry data to reveal personal preferences)

Table 3. Main questions posed to participants to inform quantitative analysis of overall concerns of CPIC, and the open text question used to inform qualitative analysis

Product Risks and Causes.

Product Risks and Causes	
Specific Risk Concern To what extent are you concerned about the following potential risks that might be associated with this product? *(Not concerned at all to Extremely concerned)*	**Data security** (eg: Privacy, Improper Information Storage/leakage, Hacking) **Psychological** (eg: anxiety – fear of product failure, increased stress) **Social relationships** (eg: Decreased face-to-face communication) **Equipment safety** (eg: Equipment Failure, Improper Operation) **Physical health** (eg: injury, Sleep disturbance)
Cause Type To what extent do you think the following factors lead to the potential risks associated with this product? (*Does not lead at all to Completely leads)*	Design flaw or malfunction Data leakage or privacy issues Improper use or Malicious operation Inadequate warnings or instructions

Participants were then randomly presented with five of the ten products to rate, and asked to assume that they owned the product if they did not already. Each product was rated on a series of nine characteristics, using a 7-point Likert scale presented in a randomised order[2]. Risk characteristics were largely selected on the basis of their use in previous

[2] There may be a concern that the way the labels at the end of each Likert scale may be leading in such a way as to prime participants to respond towards the higher end of each scale. The present study used standard measures in order to make the findings comparable to previous risk perceptions research which has a long history of using the same measures to determine public perceptions of risk. Also, as was revealed in the analyses, we do not show that all participants give ratings that are consistently on the higher end of the Likert scale, in fact they differentiate by CPIC, where some show much lower ratings (e.g. 1 or 2 on the scale), this suggests that the full range of intervals on the scale were used.

psychometric studies of consumer products (Jenkins et al., 2024; Vaubel & Young, 1992a; Wogalter et al., 1986, 1987; Young et al., 1992; Young & Laughery, 1994) and in relation to attributes of smart products (e.g., use of data). The complete list of characteristics and response scales can be found in **Table 2**.

After this, participants were asked to indicate what the biggest risk they could envisage being associated with the product, in a free text response (see **Table 3**). On a separate page, they were then asked to indicate their level of concern about specific risks, and then the degree to which various factors were perceived to lead to the potential risks associated with the product, both on 7-point Likert scales (see

Table 3). Finally, participants were thanked, debriefed, and given a code to claim their payment.

Results

All analyses were run using R (R Core Team, 2022) in R Studio, version 4.2.2 (2022-10-31) (Posit Team, 2022). The findings are organised in according with the five research questions that this study was designed to address.

1. How Are Risks Associated with Consumer Products with Internet Connectivity Perceived?

Participants rated five randomly presented products on a series of nine characteristics, see Table 2. A correlation matrix was created, featuring all of these variables, in order to check that all of the variables had at least one correlation where $r \geq 0.3$ (Tabachnick & Fidell, 2001). All of the variables did and thus were retained for the primary analysis. A principle component analysis (PCA) was subsequently conducted on the aggregated data, using a Varimax rotation. This revealed a two-component solution, explaining 89.3% of the variance (see Table 4). The first component termed **concern** (50.2%) consisted of 'worry' (extremely worried), 'control' (no control at all), 'concern' (extremely concerned), and 'consider risk when purchasing' ('would consider a lot'). The second component termed **benefits** (39.1%) consisted of 'familiarity' (extremely familiar), 'frequency of use' (daily), 'knowledge of risk' (known precisely), benefit (very great benefit), 'vulnerable groups interaction' (completely disagree). Higher scores on the concern component were positively correlated with scores on the benefits component, indicative of high levels of risk tolerance.

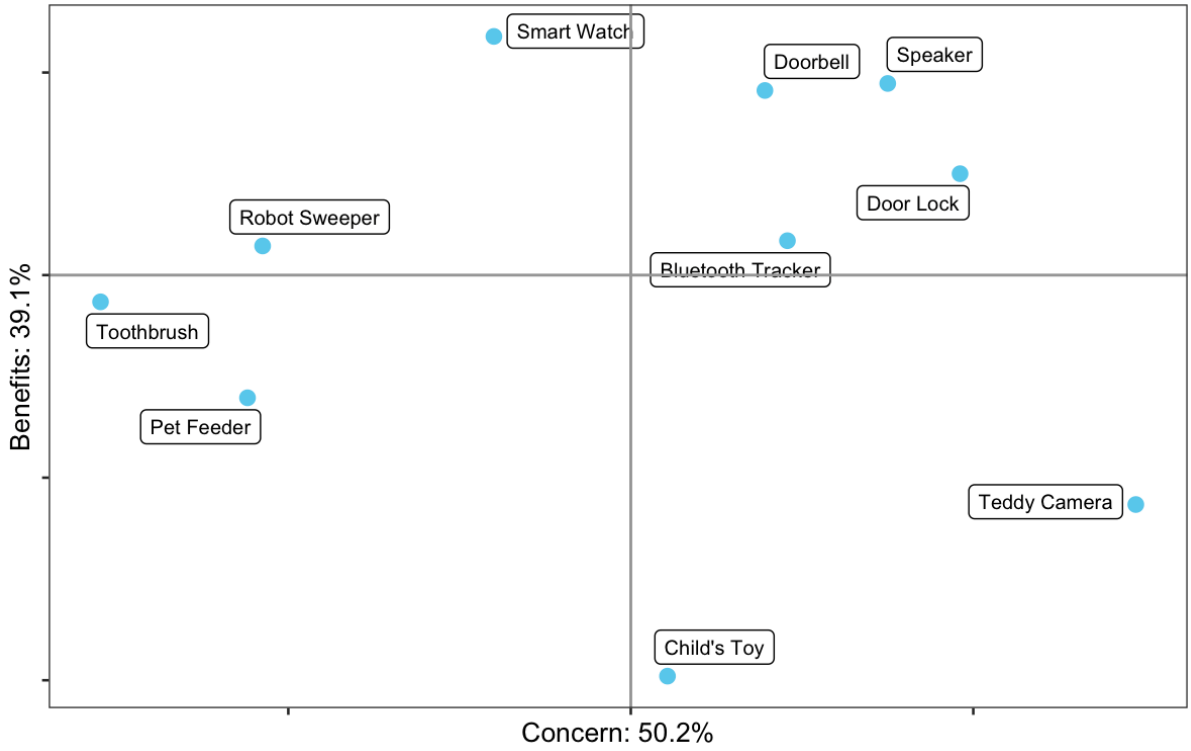
Table 4. Presentation of outcome of the Principal component analysis conducted on aggregated data from the key 9 product risk ratings

Loadings from the PCA – Aggregated Data

Characteristic	**Component**	
	Concern (50.2%)	Benefits (39.1%)
Worry	**.956**	
Control	**-.978**	
Concern about data usage	**.980**	
Consider risk when purchase	**.939**	-.171
Familiar		**.854**
Frequency	-0.518	**.768**
Benefit	-.496	**.822**
Knowledge of risk	0.101	**.949**
Vulnerable groups interaction	0.524	**-.734**

Figure 1 Risk map of the two components (concern, benefits) for the 10 CPIC

Location of Products Within the Benefits and Concern Component Space



2. What Personal Characteristics Predict Risk Perceptions of Consumer Products with Internet Connectivity?

Having identified these two dimensions underlying risk perceptions, we performed structural equation modelling (SEM) to predict concern and benefits scores derived from the PCA from the personal characteristics measured in the study using the BRMS package (Bürkner, 2017). For full model specification, see Supplementary Materials 3. Essentially, the aim here is to look at the extent to which group differences (i.e. age, gender, whether the participant has children) and general attitudes to CPIC technologies (i.e. trust in the CPIC technologies, importance of CPIC technologies in daily life) were differentially associated with the two components (concern, benefits) across all CPIC products; these two components were derived from the PCA analysis.

When it came to the component concern, only age and attitudes regarding the importance of CPIC products to one's life clearly predicted concern levels. That is, the older one is, or the more important CPIC products are to one's daily life, the lower the concern levels. When it came to the benefits component, more demographics and attitudes predicted the level of overall benefits across the 10 CPICs. As age increases benefits from CPIC lowers, females compared to males attributed lower benefits to CPIC, and those without children also saw fewer benefits of CPIC compared to those with children. Attitudinally, the more important CPIC products are seen as important in daily life, and as trust increases, so too does perceived benefits (see

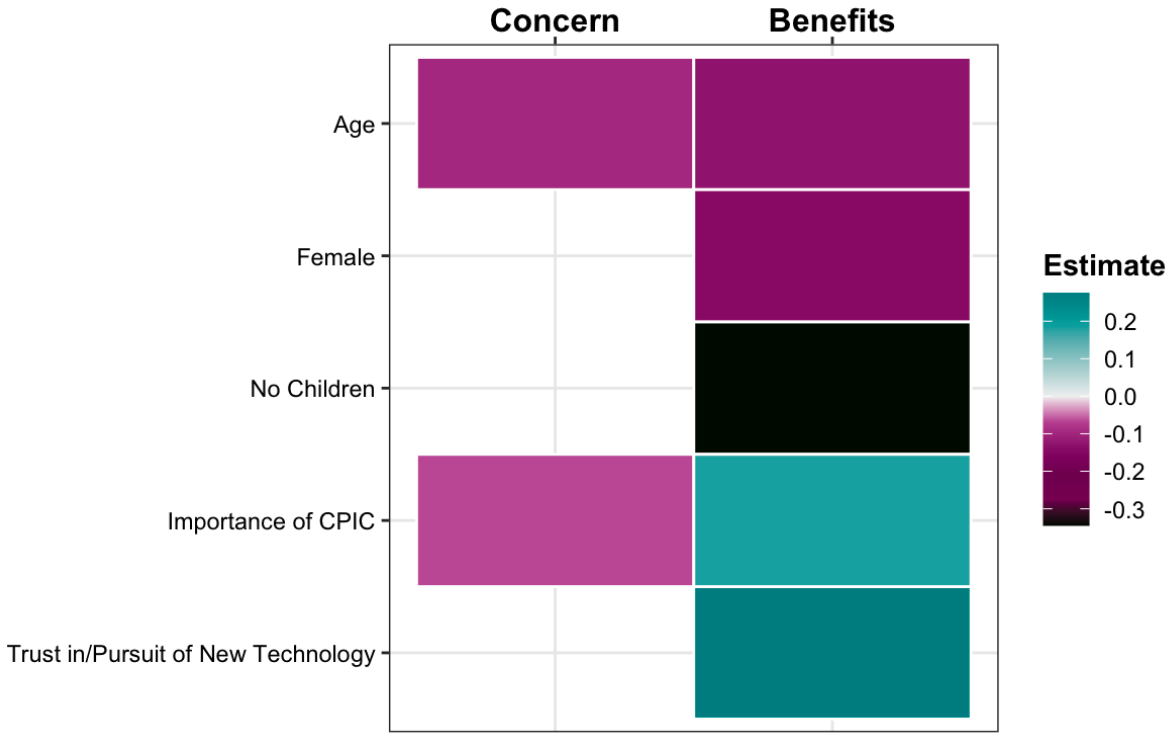


Figure 2).

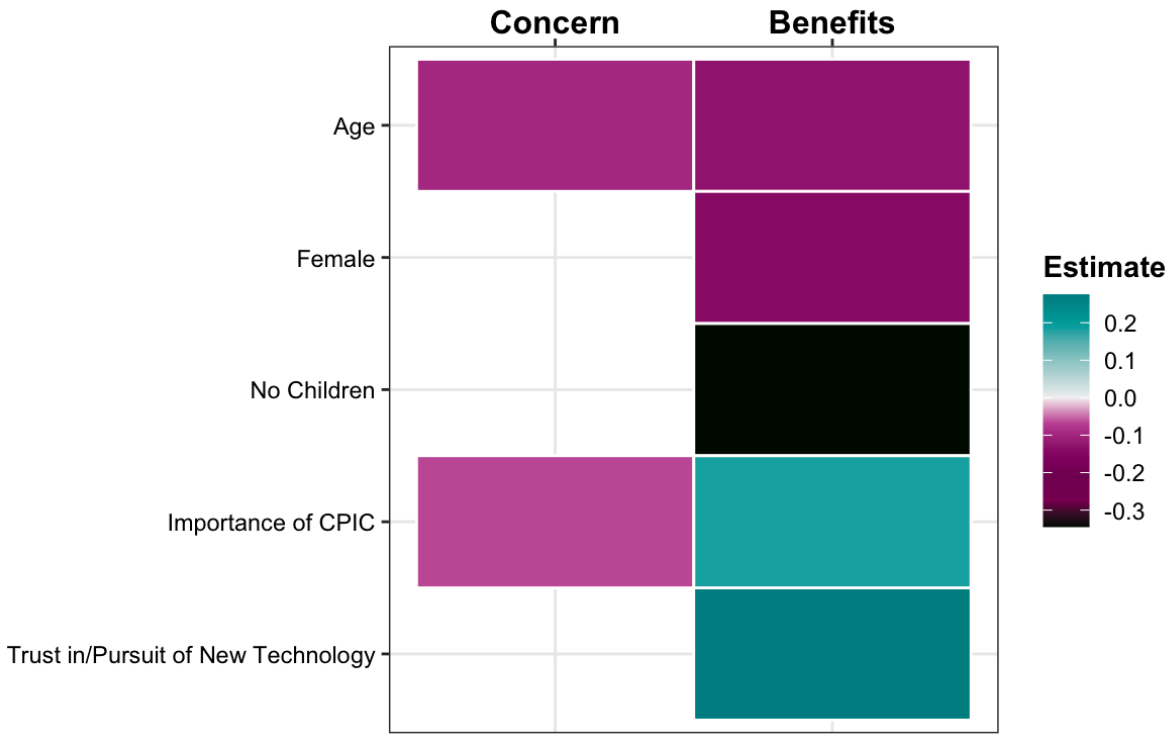


Figure 2 Visualisation of demographics and general attitudes to CPIC and their relationship to concern and benefits components.

The colour shading here is from black to magenta to green, with green indicating positive loadings and black to magenta indicating negative loadings. The blocks of colour against the demographics (age, gender, having children) and attitudes (importance of CPIC, Trust) indicate which ones strongly predicted either concern or benefits. Clear (≠ 0) Predictors of risk perceptions. The final model specified was: Concern, Benefits ~ (Age + Gender + Children + Importance of CPIC + Trust/Pursuit New Technology) + (1|product) + (1|ID)). Positive (negative) estimates indicate high (low) concern, high (low) benefits.

Risk Tolerance and Intensity

As has been noted in previous literature, risk perceptions are only part of the equation when it comes to whether an individual will take action or not in light of a risk; what matters more is an individual's risk tolerance – the trade-off they make between perceived risk and perceived benefit (Jenkins et al., 2024; Office for Product Safety & Standards, 2024). Its complement is *risk intensity* – the overall perceived potency of a risk. In the current context, we propose risk tolerance represents to decision to pursue a smart product and its associated

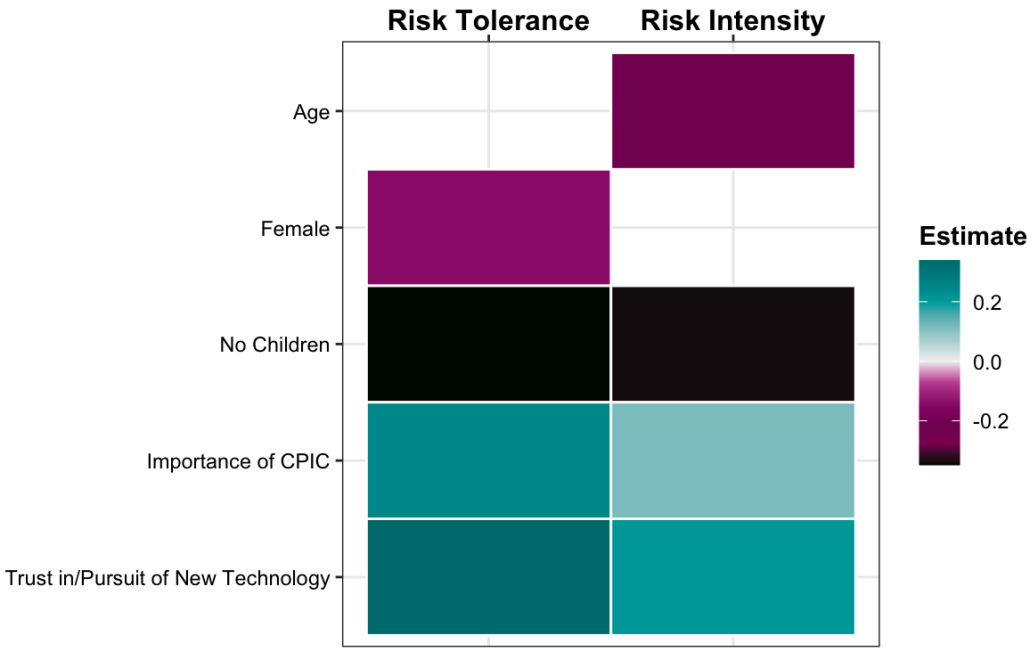
risks, given the benefits afforded by it, and is calculated by benefits minus the concern dimension. Risk intensity is calculated by summing the benefits plus concern dimension.

Using the same methodology for predicting risk perceptions, we performed structural equation modelling (SEM) to predict risk tolerance and intensity. For full model specification, see Supplementary Materials 2.

For both risk tolerance and risk intensity were predicted by the importance of CPIC to one's life, as well as trust in/pursuit of new technology – the more important/more trust in new technology. In short, for both these measures of general attitudes towards CPIC, the higher the positive attitude to CPIC technologies the higher the risk tolerance and intensity perceived. Females and those with no children we see that they had lower levels of risk tolerance. Also, we also see that for risk intensity, as age increases, and for those with no children then the lower the perceived risk tolerance and risk intensity (see Figure 3).

Figure 3. Presentation of demographics and attitudes and the loadings on the two components (concern, benefits)

The colour shading here is from black to magenta to green, with green indicating positive loadings and black to magenta indicating negative loadings. The blocks of colour against the demographics (age, gender, having children) and attitudes (importance of CPIC, Trust) indicate which ones strongly predicted risk tolerance and risk intensity. Clear (≠ 0) Predictors of Risk Tolerance and Intensity. The final model specified was: Risk Tolerance, Intensity ~ (Age + Gender + Children + Importance of CPIC + Trust/Pursuit New Technology) + (1|product) + (1|ID)). Positive estimates indicate increased risk tolerance and intensity.



3. Do Individuals Distinguish Between Different Types of Risks Associated with Consumer Products with Internet Connectivity?

Participants were asked to rate their level of concern for five different types of risks associated with CPIC. A 5 (risk type) × 10 (product) revealed a significant main effect of risk type, $F(4, 19722) = 1245.96$, $p < .001$, $\eta^2p = 0.20$, a main effect of product, $F(4, 19722) = 195.19$, $p < .001$, $\eta^2p = 0.08$, which were qualified by a significant interaction $F(36, 19722) = 60.21$, $p < .001$, $\eta^2p = 0.10$. We took a simplified approach to following up this significant interaction and examined each product individually (see Supplementary materials), for three main reasons: (a) given the large number of post-hoc comparisons and associated loss of power, (b) the fact that we did not have a priori expectations about how the products would differ, given their selection was intended to reflect what was available on the market, (c) few prior studies provide analyses at the level of individual CPIC products, instead the findings are usually collapsed across products to show overall attitudes and perceptions of smart homes of which the products constitute (He et al., 2019l Klobas et al., 2019; Shank et al., 2021).

Overall, to summarise the key findings, the individual analyses performed for concern ratings for each of the 10 CPICs included in the present study show that there was a significant effect of each of the five risk ratings (equipment safety, psychological harm, data security, physical health, social relationships) on ratings of concern. There was variation in terms of which risk factor was associated with the highest level of concern which is presented in Table 5. What Table 5 reveals is that of the 10 CPICs, the highest concern for 6 of them was data security, which is consistent with much of the literature that has previous examined users experiences and general attitudes towards CPICs (e.g., Chalhoub et al., 2021; Denning et al., 2009; Klobas et al., 2019; Shank et al., 2023; Wilson et al., 2015, Wilson et al., 2017). The risk factor that presented the lowest concern overall for 7 out of the 10 CPIC was social relationships. With regards to psychological harm (see supplementary materials) across all 10 CPIC, we see that of all 5 risk factors, it appears consistently in the middle range with respect to concerns, that is, it is neither the highest nor lowest of concern of all 5 risk factors.

Table 5. Summary of the risk factors that present as the highest and lowest of concern for each individual CPIC

Summary of Risk Types Associated with Highest and Lowest (Significantly Different) Concern Ratings by Product

Product	Concern Rating	
	Highest	**Lowest**
Pet Feeder	Equipment Safety	Physical Health/ Social Relationships
Speaker	Data Security	Social Relationships/ Physical Health
Teddy Camera	Data Security	Physical Health/ Social Relationships
Child's Toy	Data Security	Physical Health
Doorbell	Data Security	Social Relationships/ Physical Health
Toothbrush	Equipment Safety/ Data Security	Social Relationships
Bluetooth Tracker	Data Security	Social Relationships/ Physical Health
Door Lock	Data Security/ Equipment Safety	Social Relationships
Robot Sweeper	Equipment Safety	Social Relationships
Smart Watch	Data Security	Physical Health/ Social Relationships

4. Do Individuals Distinguish Between Different Causes of Risks Associated with Consumer Products with Internet Connectivity?

Participants were asked to the extent to which they thought four factors (i.e., Design flaw or malfunction, Data leakage or privacy issues, Inadequate Warnings or Instructions, Improper Use or Malicious Operation) caused the risks associated with CPIC. A 4 (cause type) $\times$ 10 (product) revealed a significant main effect of cause type, $F(3, 15779) = 263.31$, $p < .001$, $\eta^2p = 0.05$, a main effect of product, $F(9, 15779) = 167.56$, $p < .001$, $\eta^2p = 0.09$, which were qualified by a significant interaction $F(27, 15779) = 60.21$, $p < .001$, $\eta^2p = 0.08$.

As before for concern ratings (RQ3), we took a simplified approach to following up this significant interaction and examined each product individually (see supplementary materials for all comparisons for each CPIC), for two main reasons: (a) given the large number of post-hoc comparisons and associated loss of power and (b) the fact that we did not have a priori expectations about how the products would differ, given their selection was intended to reflect what was available on the market. Table 6 summarises the analyses conducted for each of the 10 CPIC in the study. For 7 out of the 10 products, data leakage and privacy issues as causes of issues for CPIC are the highest rated causes for concern. For 8 out of the 10 CPIC inadequate warnings or instructions as causes of issues for CPIC present the lowest level of concerns relative to the other three causal factors presenting risks to users.

Table 6. Summary of ratings of the four causal factors (Design flaw or malfunction, Data leakage or privacy issues, Inadequate Warnings or Instructions, Improper Use or Malicious Operation) and their relationship to ratings of concern.

Summary of Highest and Lowest (Significantly Different) Ratings of Cause Type by Product

	Cause	
Product	**Highest Rated**	**Lowest Rated**

Pet Feeder	Design Flaw or Malfunction	Data Leakage or Privacy Issues
Speaker	Data Leakage or Privacy Issues	Inadequate Warnings or Instructions
Teddy Camera	Data Leakage or Privacy Issues/ Improper Use or Malicious Operation	Inadequate Warnings or Instructions
Child's Toy	Data Leakage or Privacy Issues/ Improper Use or Malicious Operation	Inadequate Warnings or Instructions
Doorbell	Data Leakage or Privacy Issues	Inadequate Warnings or Instructions
Toothbrush	Design Flaw or Malfunction	Inadequate Warnings or Instructions/ Data Leakage or Privacy Issues/ Improper Use or Malicious Operation
Bluetooth Tracker	Data Leakage or Privacy Issues/ Improper Use or Malicious Operation	Inadequate Warnings or Instructions
Door Lock	Data Leakage or Privacy Issues/ Improper Use or Malicious Operation	Inadequate Warnings or Instructions
Robot Sweeper	Design Flaw or Malfunction	Inadequate Warnings or Instructions/ Data Leakage or Privacy Issues/ Improper Use or Malicious Operation
Smart Watch	Data Leakage or Privacy Issues	Design Flaw or Malfunction/ Inadequate Warnings or Instructions

5. What Kinds of Concerns Do People Volunteer When Thinking About Consumer Products with Internet Connectivity?

To answer this questions, 4648 self-reports were examined that include descriptions of concerns participants had with specific smart products. To analyses this qualitative data required designing a coding frame for broad and granular level analyses. A coding frame was

used to classify the free text into superordinate and then subordinate categories. The steps taken to achieve this were guided by recommendations (e.g. Blair, 2015; Elliott, 2018; Skjott Linneberg & Korsgaard, 2019) that are well-regarded by many qualitative researchers.

Initial Screening

An initial screening was used to label text that could not be labelled as 'Uncoded'. This was for two reasons. The text was unreadable because it had been corrupted when opened in another application (e.g. "ä¼šæš^^^"), or because the concern described was too broad or vague to be adequately related to a specific concern or a specific product (e.g. "AI is taking over the world"). While screening, it was also clear that a non-trivial number of participants did not have any concerns and explicitly indicated that they did not think that the product posed any risks, this text was labelled 'No concerns'. Also, some participants indicated they weren't sure, didn't know, or did not know enough to be able to confidently describe what their concerns could be, these responses were labelled 'Don't know'. The results of this initial screening process are presented in

Table 8.

Table 7. Initial Screening of self-reports

Initial Screening Process Details

Screening Process (Total responses n= 4648)				
Conditions for exclusion from full coding of response n (%)				
Failure to respond to other questions in survey	Ambiguous or uninterpretable	Unsure or don't know	Explicitly indicated no risk	Total screened from full coding
127 (3.1%)	57 (1.4%)	37 (0.9%)	184 (4.5%)	405 (9.9%)

First Open Coding of Responses

After the screening, an open coding approach was taken which involves careful reading of the free text, in this case line by line, to detect high level groupings (Blair, 2015). The motivation was to find general enough patterns that lead to minimal exclusion of the data, and could be used for statistical analyses. This produced two high level groupings: one which supported labelling of the text by the *number of concerns* generated, and the other which revealed the superordinate category *product functioning*.

The second procedure began from scratch with an opening coding approach reviewing each individual line of text using a clean version of the data set without any label or category structure that was revealed in the first procedures. This helps to ensure that there is a reliable mapping of any coding of qualitative data, and can be used to check consistency across different coding levels (e.g. superordinate, sub-ordinate) (Elliott, 2018). This time the focus was on reviewing the text by generating labels that could accurately and succinctly capture the essence of the concern, for every individual concern that was generated. This was also a way to check the consistency in the way the free text was labelled according to the number of concerns generated by each participant for each product they described a concern for, and

whether there were multiple concerns contained with a description, and whether they were separate or conditional on each other. The coder performed this labelling without consulting any of the details of the study protocol or knowledge of the specific quantitative judgement questions that were presented either side of the free text question.

When it came to open coding, two aspects of the free text emerged. The first related to the number of concerns generated, and the second related to product functioning – whether normal or abnormal.

Superordinate Category: Number of Concerns Generated

Participants did one of three things:

(1) They provided details of a single concern with respect to a smart product, for instance that it could malfunction, or that it could invade privacy. For example, Unique No. 6. [smart pet feeder] "*A product malfunction could mean that the pet is over fed. This could lead to health consequences for the pet*." Unique No. 662 [smart speaker] "*I would worry that it is listening to every single thing spoken*."

(2) Other participants provided multiple concerns. For some, this involved describing separate issues relating to a specific smart product, for instance invasion of privacy and that the product could malfunction because of poor internet connectivity; For example, Unique No. 1624 [Smart teddy bear camera] "*This would depend on the level of security the parent set up within the toy, but it could pick up conversations. It would reduce the amount of physical contact the child had with other people*", Unique No. 3256 [Smart Door lock] "*Wifi, battery or fob failure resulting in being locked out. Easier to hack into than with a key*."

(3) In other cases, participants described multiple concerns that were conditional on each other. For example, when describing the possibility that a smart product could be hacked, this was followed by a description of a criminal activity that could occur once the product was

hacked. For instance, Unique No. 1602 [smart vacuum cleaner] "*The robot is connected to the internet which means it can be hacked and leak personal information*.", Unique No. 2779 [smart fitness tracker] "*The biggest risk I could envision associated with this product is that it could be used to track people's movements without their knowledge. This could be used for stalking, harassment, or even kidnapping*."

As such, the first superordinate category simply classified the free text to one of three categories: (1) Single; (2) Multiple separate; or (3) Multiple conditional concerns. Separating the free text in this way also helped to identify which were the primary concerns, which were taken to be the concern articulated first, and of course for multiple conditional concerns, where the second concern was conditional on the first issue occurring. For a full breakdown, see

Table 8.

Superordinate Category: Product Functioning

The second pattern that emerged informed the second superordinate category structure 'product functioning' (see

Table 9). Concerns were described even when the product was assumed to be functioning normally. More specifically, the product could operate normally but was still described as presenting concerns regarding data harvesting (e.g., collecting data on pet food consumption rates) or privacy (e.g., it is always eavesdropping in conversations). For example, Unique No. 1587 [smart children's toy] "*The only risk is that there is a chance of data harvesting if there is subscriptions that have to be set up to use the product*.", Unique No. 99 [smart pet feeder] "*I would be worried my pets wasn't getting fed or watered enough. I wouldn't rely on it at all*.", Unique No. 511 [smart speaker] "*Eavesdropping on private conversations and monitoring activities without consent*". Note also that the concerns were labelled as pertaining to the normal functioning of the product unless explicitly stated otherwise. Where participants did refer to the abnormal functioning or product failing, they did this in two ways – either it could malfunction, or it could fail to provide sufficient data security or data protection measures.

In some descriptions, participants identified concerns based on the product malfunctioning (e.g., being electrocuted from product malfunction) or the causes that could mean a product malfunctions (e.g., batteries getting flat, or overheating). For example, Unique No. 2216 [smart toothbrush] "*If not well manufactured, it could lead to an electric shock*", Unique No. 3914 [smart watch] "*Overheating of the battery, charging risks when plugged to power*.", and Unique No. 1451 [smart children's toy] "*Lithium-ion batteries getting hot under charging*".

The third overarching concern related to unauthorised access to the home network because of poor data security protections that could then lead to a device being hacked or data being leaked. In this case, the physical product performs its functions as expected, but the "smart" component of the product is not providing sufficient protections. For example,

Unique No 1044 [smart teddy camera] "*Perverts being able to access live feeds by way of weak security settings would be of worry to me*", Unique No. 3144 [smart door lock] "*Security issues - what if someone hacks it and is able to enter*", Unique No. 2007 [smart doorbell] "*The security of the app/device being compromised that criminals could possibly exploit*".

Therefore the second coding of the free text was based on categorising the descriptions according to whether the concern was primarily referring to: (1) *Normal functioning* – the product operating as intended; (2) *Malfunctioning* – that includes concerns about what could cause, or what could result in the product failing to operate as intended; or (3) *Unauthorised access* – that includes examples of activities that result from insufficient data security and data protection measures of the smart functionality of the product.

Table 8. Summary of the Final Set of Coded Responses, Including Number of Concerns and Those Individual Concerns Classified Under the Main Superordinate Category 'Product Functioning'

	Type of Coded Response				
†Total no. of free text responses (n = 4243)	A single concern was volunteered	A single free text response volunteered multiple separate concerns were volunteered		**‡**A single free text response volunteered multiple concerns that were conditional on each other	
Total No. of individual coded concerns (n = 5069)	2287 (45.1%)	1128 (22.3%)		1654 (32.6%)	
	2287	564 1st concern	564 2nd separate concern	827 1st concern	827 2nd conditional concern
Product Functioning Classification					
Normal functioning (n = 2988, 59%)	1378	372	360	490	388
Malfunctioning	386	81	62	31	20

(n = 580, 11.4%)					
Unauthorised access (n = 1501, 29.6%)	523	111	142	306	419

†This refers to the total number of free text responses that remained once screening was applied (e.g., Unintelligible, Don't knows/Unsure, No risks/concerns, Excluded from other analyses).

‡ In some cases, the free text responses included multiple concerns. Some participants volunteered two separate unrelated concerns related to a particular smart product. Other participants reported multiple concerns where one concern in turn led to a further related concern that was conditional on the first occurring. The two types of multiple concerns were classified separately.

Second Open Coding of Responses

Subordinate Category - Specific Concerns

The second open coding of the free text involved labelling the concerns by using a succinct phrase or term which could then standardise the concern being referred. It was clear from the labels, that they could be grouped into four broad categories that were mutually exclusive, at least in how the concerns were described, that fell under the subordinate category of 'Specific Concerns'. The subordinate categories are: (1) Concerns of a psychological nature; (2) Concerns around criminal activity and malicious behaviours; (3) Concerns around data and (4) Concerns around physical outcomes. The different types of labelled concerns falling under each of the four superordinate categories are presented in

Table 9. For instance, participants described concerns that related to “listening in”, “eavesdropping”, “privacy issues”, “overhearing personal conversations”, and “always watching”. Descriptions of concerns that contained these or other related phrases were labelled “Invasion of privacy/Privacy concerns”.

To illustrate, regarding concerns that refer to psychological impact, we see the three different types (See Table 9) primarily referred to with respect to CPIC that were designed for children. In fact 52% (n = 116) of the psychological related concerns were for the smart teddy camera (n = 10) and the smart children’s toy (n = 106). With respect to adverse emotional impacts, we see a range of similar concerns, Unique No. 1438 [smart children’s toy] “*lack of human touch or humanity, machines do not have empathy*”, Unique No. 1440 [smart children’s toy] “*Lack of Personal interaction. No emotional connection*.”. But we also see this being discussed with respect to other products, for example Unique No. 86 [smart pet feeder] “I feel there’s a bond with your pets, especially and feeding times. If you can’t feed your pet, you shouldn’t have one!”. Concerning the adverse cognitive impacts, they are exclusively referred to in association with the smart children’s toy. For instance, Unique No. 1292 “*Could potentially teach them inappropriate words, or teach them the wrong stuff*.”, Unique no 1509 “*Robot brain washing child with a certain programming*”, and Unique No. 1607 “*The robot may not understand the child’s issues or learning speed and style. Some children may develop at a different speed. Can the robot identify learning problems such as dyslexia? There's a risk that the robot will treat everyone the same and not be able to differentiate*.”. When it came to behavioural impacts, we see a range, which is also why they are referred to across all 10 types of CPIC, as compared to emotional and cognitive impacts. To illustrate, Unique No. 4074 [smart watch] “*When out and about you are so engrossed in looking at this device you don't notice what is around you & could have an accident*.”, Unique No. 2365 “*That it might induce*

an obsession with cleaning that goes beyond what is required. I don't really think it is a risky product though.", Unique No. 3527 [smart vacuum cleaner] "*Perhaps making a person more indolent. Sometimes exercise through cleaning is the only exercise for the very old*?" and Unique No. 2064 [smart toothbrush] "*Become obsessed with tracking the results and over-analysing any statistics. Could lead to OCD obsessions*.". The aim here is to show that psychological impacts contain several distinct types that need to reflect the descriptions which reveal important nuances.

When it came to specific examples of criminal activity, we see that descriptions of them span all 10 products, and this applies with respect to criminal activity in the physical domain, which is treated in this analysis as separate from criminal activity in the digital domain. To illustrate, Unique No. 3121 [smart door lock] "*People stealing access and getting into the house or other things protected by the lock*", Unique No. 2911 [smart door lock] "*Could be accessed by others and used to gain illegal access, could be used to find a pattern of when the house is empty"*, Unique No. 1964 [smart doorbell] "*Someone using it to find out you're not at home because you don't answer the door even though the smart doorbell is working, and so they break into your house*.", Unique No. 3881 [smart watch] "*Location data tracked by criminals to know my movements in order to burgle my house/mug me when out running in a remote area*" and Unique No. 867 [smart teddy camera] "*could be used for recoding information used for blackmail or harassment."*. These are distinct from criminal activity in virtual domain, such as, Unique No. 963 [smart teddy camera] "*Ill intended people can access it remotely and spy on you , or your child*.", Unique No. 1107 [smart teddy camera] "*someone remotely can film my family without my knowing*.", Unique No. 2515 [smart fitness tracker] "Could be used to stalk or track people", Unique No. 3541 [smart vacuum cleaner] "*potential personal data being stolen from device*".

The third area specific concern was around data, most often data privacy issues, and again we see that the descriptions of the concerns participants had spanned all 10 products, though data privacy was the referred to most frequently with respect to the smart speaker (33%) and the smart teddy camera (15%). For instance, Unique No. 799 [smart speaker] "*They listen and speak when not called on. Data is stored from our general conversations*.", Unique No. 932 [smart teddy camera] "*I think it can threaten privacy and cause problems on the family.*, Unique No. 2367 [smart fitness tracker] "*Lack of privacy in terms of monitoring my movements*.", and Unique No. 4082 [smart watch] "*Zero privacy, collects personal data*."

There were many other data concerns which have been illustrated earlier, but to give a sense of the range, examples here include third party access (Unique No. 682 [smart speaker] "*Potentially taking your data and sharing it to other people*."), data protection (Unique No. 1788 [smart doorbell] "*if image stored in cloud, who has access to it, how secure is it*", data security (Unique No. 364 [smart pet feeder] "*The connectivity to a smart device may pose security risks through malware*."), incorrect information provided (Unique No. 453 [smart speaker] "*Could give wrong answer/information leading to harm*."), data leaks (Unique No. 1840 [smart doorbell] "*leaking of footage or location data*.", and gaining access to control other devices (Unique No. 681 [smart speaker] "*Potentially could be [hacked] into, so people can use them to control and access your connected devices*").

Table 9. Frequency of concerns that were coded into the subordinate category 'Specific Concerns' (Psychological, Criminal & Malicious, Data issues, Physical outcomes)

Specific Concerns (n = 4627)							
Psychological (n = 229) (5%)		**Criminal activity and malicious behaviours** (n = 1267) (27%)		**Data issues** (n = 2612) (57%)		**Physical outcomes** (n = 519) (11%)	
Negative behaviour change	117	Cybercrimes (e.g., cyberstalking/cyber surveillance, data theft, hacking)	741	Invasion of privacy/ privacy concerns	781	Physical harm	413
Negative emotional impact	62	Malicious intentions	245	Data harvesting	775	Property damage	63
Negative cognitive impact	50	Specific crimes mentioned (e.g., burglary, child sexual crimes, home invasion, blackmail, domestic abuse, kidnapping)	213	Unconsented third party access & spamming	366	Fire hazard	37
		Criminal activity (i.e., generic description of criminal activity)	36	Data protection issues/ data security	289	Damage/ malfunction	6
		Financial harm	31	Improper or incorrect information provided	186		
				Data leaks	125		
				Access to other devices and control of them	100		

Discussion

Using a mixed methods approach, the present exploratory study was designed to address the following research questions: (1) How are risks associated with CPIC perceived? (2) What personal characteristics predict risk perceptions of CPIC? (3) Do individuals distinguish between different types of risks associated with CPIC? (4) Do individuals distinguish between different causes of risks associated with CPIC? and (5) What kinds of concerns do people volunteer when thinking about CPIC?

We found that consumer risk perceptions of CPIC comprise of two components: concern and benefits. Risk characteristics such as worry, concern and lack of control over the risk formed the basis of the concern component, which is akin in sentiment to the dread component identified in recent psychometric studies of consumer products (Jenkins et al., 2024; Office for Product Safety & Standards, 2024). Notably, the primary component explaining most variance in risk perceptions in previous studies has typically been more neutral (e.g., familiarity [Vaubel & Young, 1992]; (un)known [Feng et al., 2010; Young & Laughery, 1994]) or even positive in sentiment (e.g., benefits [Jenkins et al., 2024; Office for Product Safety & Standards, 2024]). In contrast, for CPIC, concern was the largest component, with benefits second, possibly reflecting consumer apprehension about these types of products. This aligns with previous research which has found with smart functionality are perceived as more risky than their non-smart counterparts (Hunte et al., 2024; Rijsdijk & Hultink, 2003, 2009). Looking at the spread of products across the component space (Figure 1), those that were perceived as most beneficial (door lock, speaker, doorbell, Bluetooth tracker) could feasibly be described as smart versions of household goods, appliances or healthcare (as opposed to leisure, recreation or personal care products (e.g., Jenkins et al., [2024]; Office for Product Safety & Standards [2024]). They were, however, also perceived as

some of the most concerning, alongside those perceived as relating particularly to children (teddy camera, child's toy).

Following the ICONS framework (Jenkins et al., 2024), we also sought to explore the role of individual characteristics in shaping risk perceptions, finding that the socio-demographic factors age (older), gender (females) and parental status (no children) were predictive of (fewer) benefits, and older age predictive of lower levels of concern. This was largely in keeping with results from Jenkins et al. (2024) who examined consumer products *without* internet connectivity, aside from the direction of the gender effect on benefit perceptions. However, if one purely analyses the difference in ratings on the 'benefit' characteristic (rather than component) between males and females, there is no significant difference (p = .86), suggesting other characteristic loadings could be driving this predictive effect of gender on benefits.

It is unsurprising that attitudes also influenced perceptions, with importance of CPIC predictive of lower levels of concern, and both importance and trust in new technology predictive of higher levels of benefits. Essentially, positive views of such technology/products have a protective effect, which is further reflected in the analysis of predictors of risk tolerance. Risk tolerance refers to the notion that consumers trade off risks and benefits in order to define an acceptable level of risk, which can then be used to predict information seeking/sharing and behaviour (Jenkins et al., 2024; Office for Product Safety & Standards, 2024). Given the vast benefits afforded by CPIC, in combination with the significant levels of concern displayed, it is an exceedingly pertinent concept in the context of CPIC (Hunte et al., 2024; Osman, 2025a). Crucially, those who placed a great deal of importance on CPIC and trust in new technology demonstrated higher levels of risk tolerance with such products –

further emphasising the need for risk management efforts to consider not just the public's risk perceptions, but also their tolerance of the associated risks.

The types of risks perceived seemed to be broadly consistent across different types of products, with data security concerns being the most common. This finding is aligns well existing research on security breaches and privacy intrusions as one of the most common forms of harm in smart homes (Buil-Gil et al., 2023; Osman, 2025b). In addition the present findings complement work showing that the predominant concerns reported by users (e.g., Adeyeye 2024; Cannizzaro et al. 2020; Chan-Olmsted, Chen, and Kim 2024; Cobb et al. 2021; Haney and Furman 2023; Jaspers and Pearson 2022; Korneeva, Olinder, and Strielkowski 2021; Schomakers, Biermann, and Ziefle 2021; Turner et al. 2022) are related to privacy (Chhetri & Motti, 2022; Nicholson et al., 2025). Our findings also speak to the potential for smart technology to have adverse effects on social interactions and development of social/emotional skills (OECD, 2019). The analysis of quantitative data from the present study does to support this. While there are some concerns that align with the potential impact of CPIC on social interactions (e.g. that the product is viewed as a substitute for a care giver to their child, or between pet owner and pet), examples like described in the self-reported concerns made up 27% of the overall the psychologically themed concerns, which in turn made up 5% of the overall concerns reported.

As CPIC continue to become more popular and widespread, many countries are extending their regulatory and legislative efforts to encompass such products, for instance: the UK's Product Security and Telecommunications Infrastructure Act (2022); the EU's Cyber Resilience Act (2024); the EU REGULATION (EU) 2023/988 on General Product Safety (2023); China's Regulations on the Management of Security Vulnerabilities in Network Products (2021). In some instances, these efforts include explicit reference to psychological harm

(albeit without a clear definition), but despite the term gaining traction, we find that psychological harm remains virtually absent in the public's awareness. Instead, the majority of concerns articulated related to data issues (57%), criminal activity/malicious behaviours (27%), physical outcomes (11%) and lastly psychological concerns (5%). Whilst it has been suggested that previous findings of psychological harm ranking low in the public's minds could be a reflection of methodological constraints (e.g., in how the term is defined, or measured, Osman, 2025b), in this study participants had completely free rein to volunteer their concerns. The fact that consumers rarely, if ever, freely express concerns about psychological harm in any great numbers further reinforces previous research suggesting that it is simply not a priority to them. Assuming it does risks promoting an excessively precautionary approach to regulation (Jenkins & Ayton, 2025).

Of additional note was that the free text concerns typically related to when the product functioned *as normal*, versus malfunctioning, which presents a challenge not just for consumers, but also for regulators. Historically, product safety regulations were established at a time where harms were physical, caused by, for instance, mechanical failures – that is, harm arising from unintended malfunction or misuse (Ruohnonen, 2022). Indeed, both the General Product Safety Regulations: GB (2005) and EU Regulation on General Product Safety 2023/988 (2023) state that a safe product is "one which, under normal or reasonably foreseeable conditions of use, does not present any risk or only the minimum risks compatible with the product's use…". In an era of rapid digital and technological transformation means new products are entering the market, along with new norms of usage. Consequently, regulators responsible for product safety must reconsider and reconceptualise not just what constitutes harm (Farrand, 2024) but also what it means to be safe (Ruohonen, 2022). Such shifts have implications for the ways product risks can be most effectively assessed, managed

and communicated, as well as the potential to further complicate and fragment the global regulatory landscape (Farrand, 2024).

Given that the study was motivated to provide insights from public perceptions of risks from CPIC, we can draw from the findings we present here to suggest the following potential future directions that could support policy decision-making o CPIC.

Policy Recommendations

1. There is good reason to focus on designing ways of measuring public risk tolerance as well as risk perceptions, where the former, based on emerging evidence is a better predictor of behaviour. That is, in order to develop a more accurate picture of how prospective and current users of CPIC behave with respect to CPIC (e.g. usage of CPIC, increased adoption of multiple CPIC) risk tolerance is likely to be a better predictor of behaviour than risk perceptions alone. The reason for this is that risk tolerance takes into account two practical ways in which the public are likely to evaluate CPIC and that is the overall benefits of them traded of the overall costs (e.g. concerns, worry, lack of control, privacy). To profile how the public will currently, and in the future, respond to CPIC, especially given the increase in the range and type of CPIC on the market, using risk tolerance along with measures of risk perceptions are a more comprehensive way of doing so.

2. It is critical to look at a range of CPIC and to consider how public tolerances of risk are attributed to specific CPIC rather than as smart products in the home. A more granular approach of this kind better reveals how specific CPIC could be targeted that present concerns to users. Moreover there are several taxonomies that could be used as ways of grouping the CPIC by their potential uses (e.g. leisure, personal care, domestic appliances) or by their specific smart functionalities to assess specific risk factors and causal factors that impact user concerns of different types of CPIC.

3. It is often difficult to measure the impact of any regulatory instrument or policy, and so one way to track the influence of a new regulation of CPIC, a new policy, or specific interventions such as public campaigns to raise awareness, or new warning labels on CPIC could be tracked used the types of methods presented in the present study. That is, using the dimensions of benefits and concerns, and mapping the CPICs on a risk map, by repeating this process annually it is possible to track changes over time in public risk tolerance to CPIC. Successful public campaigns may lead to reduced concerns of CPIC over time, because the public have a better understanding of how to mitigate the risks themselves. Therefore, an annual study of public risk tolerance to CPIC would reveal how risk tolerance changes over time with more familiarity with CPIC (given increasing market penetration) and where interventions from regulators and policy makers have contributed over and above general increases in familiarity with CPIC that would likely lower concerns.

4. Attention should be paid to group differences and overall general attitudes towards new technologies, as it is clear from the present study that age, gender, whether or not individuals have children, along with attitudes does differential impact the perceived benefits and concerns users have of CPIC. Along with this, and as previous work has shown, it is also worth considering the level of familiarity and frequency of use of CPIC as additional important factors when tracking risk tolerances. The value of this is that it provides richer information with respect to segmenting users and how to target them and their needs rather than treating them as a homogenous group.

Conclusion

The current study provides a baseline understanding of how consumers perceive the risks associated with CPIC, including consideration of individual differences. We find that consumers' risk perceptions are underpinned by two components: concern and benefits,

which are traded off to determine their risk tolerance of such products. Our use of both quantitative and qualitative methods yields consistent findings that concerns about CPIC are dominated by issues of data security and privacy. These results have implications for wider risk management and regulation, as we reiterate the notion that such efforts will be most effective when they align with people's concerns. We do not find evidence to suggest that consumers believe these risks simply to do with insufficient warnings or that psychological harm associated with CPIC should be at the top of the list of priorities. Future work should seek to examine the replicability of these findings, as well considering what interventions (e.g. hard – bans, fines, and soft – public campaigns, labels) are judged appropriate given the types of harms experienced from CPIC.

References

Alhakami, A. S., & Slovic, P. (1994). A psychological study of the inverse relationship between perceived risk and perceived benefit. *Risk Analysis*, *14*(6), 1085–1096. https://doi.org/10.1111/j.1539-6924.1994.tb00080.x

Anderson, C. C., Moure, M., Demski, C., & Renaud, F. G. (2024). Risk tolerance as a complementary concept to risk perception of natural hazards: A conceptual review and application. *Risk Analysis*, *44*(2), 304–321. https://doi.org/10.1111/risa.14161

Blair, E. (2015). A reflexive exploration of two qualitative data coding techniques. *Journal of Methods and Measurement in the Social Sciences*, *6*(1). https://doi.org/10.2458/v6i1.18772

Buil-Gil, D., Kemp, S., Kuenzel, S., Coventry, L., Zakhary, S., Tilley, D., & Nicholson, J. (2023). The digital harms of smart home devices: A systematic literature review. *Computers in Human Behavior*, *145*, 107770. https://doi.org/10.1016/j.chb.2023.107770

Bouder, F., Slavin, D., & Lofstedt, R. E. (2007). The tolerability of Risk. *A New Framework for Risk Management. London: Earthscan*.

Bürkner, P. C. (2017). brms: An R Package for Bayesian Multilevel Models Using Stan. *Journal of Statistical Software*, *80*, 1–28. https://doi.org/10.18637/JSS.V080.I01

Chalhoub, G., Kraemer, M. J., Nthala, N., & Flechais, I. (2021). "It did not give me an option to decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products. In *Proceedings of the 2021 CHI conference on human factors in computing systems* (pp. 1-16).

Chhetri, C., & Motti, V. (2022). “I mute my echo when I talk politics”: Connecting Smart Home Device Users’ Concerns to Privacy Harms Taxonomy. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *66*(1), 2083–2087. https://doi.org/10.1177/1071181322661114

Cohen, L., Konstantinidis, E., Osman, M. (2023). Smart products: labelling, marketing, and framing. UK Government Report. https://www.gov.uk/government/publications/smart-products-labelling-marketing-and-framing Smart products: labelling, marketing, and framing - GOV.UKDenning, T., Matuszek, C., Koscher, K., Smith, J. R., & Kohno, T. (2009). A spotlight on security

and privacy risks with future household robots: attacks and lessons. In *Proceedings of the 11th international conference on Ubiquitous computing* (pp. 105-114).

Elliott, V. (2018). Thinking about the Coding Process in Qualitative Data Analysis. *The Qualitative Report*, *23*(11), 2850–2861. https://doi.org/10.46743/2160-3715/2018.3560

Farrand, B. (2024). How do we understand online harms? The impact of conceptual divides on regulatory divergence between the Online Safety Act and Digital Services Act. *Journal of Media Law*, *16*(2), 240–262. https://doi.org/10.1080/17577632.2024.2357463

Feng, T., Keller, L. R., Wang, L., & Wang, Y. (2010). Product quality risk perceptions and decisions: Contaminated pet food and lead-painted toys. *Risk Analysis*, *30*(10), 1572–1589. https://doi.org/10.1111/j.1539-6924.2010.01459.x

Finucane, M. L., Alhakami, A., Slovic, P., & Johnson, S. M. (2000). The affect heuristic in judgments of risks and benefits. *Journal of Behavioral Decision Making*, *13*(1), 1–17.

https://doi.org/10.1002/(SICI)1099-0771(200001/03)13:1%253C1::AID-BDM333%253E3.0.CO;2-S

Gelman, A., & Rubin, D. B. (1992). Inference from iterative simulation using multiple sequences. *Statistical Science*, *7*(4), 457–472. https://doi.org/10.1214/SS/1177011136

General Product Safety Regulations 2005: Great Britain (2005). https://www.gov.uk/government/publications/general-product-safety-regulations-2005/general-product-safety-regulations-2005-great-britain

GfK. (2024). *2024 Smart Home Survey*. https://nielseniq.com/global/en/insights/analysis/2024/ownership-of-smart-home-products-doubles-in-the-uk-in-five-years/

He, W., Martinez, J., Padhi, R., Zhang, L., & Ur, B. (2019). When smart devices are stupid: Negative experiences using home smart devices. In *2019 IEEE Security and Privacy Workshops (SPW)* (pp. 150-155). IEEE. Heath, A. (2025). Commentary on 'psychological harm: What is it and how does it apply to consumer products with internet connectivity?' by Magda Osman. *Journal of Risk Research*, *28*(2). https://doi.org/10.1080/13669877.2025.2496235

He, W., Martinez, J., Padhi, R., Zhang, L., & Ur, B. (2019). When smart devices are stupid: Negative experiences using home smart devices. In 2019 IEEE Security and Privacy Workshops (SPW) (pp. 150-155). IEEE

Hunte, J. L., Neil, M., Fenton, N. E., Osman, M., & Bechlivanidis, C. (2024). The effect of risk communication on consumers' risk perception, risk tolerance and utility of smart and

non-smart home appliances. *Safety Science*, *174*, 106464. https://doi.org/10.1016/j.ssci.2024.106464

Ipsos MORI. (2020). *Consumer Attitudes Towards IoT Security*. https://assets.publishing.service.gov.uk/media/607d7e588fa8f57358f07e60/Consumer_Attitudes_Towards_IoT_Security_-_Research_Report.pdf

Jenkins, S. C., & Ayton, P. (2025). Risk and the regulatory challenges of smart consumer products. *Journal of Risk Research*, *28*(2), 149–153. https://doi.org/10.1080/13669877.2025.2496233

Jenkins, S. C., Harris, A. J. L., & Osman, M. (2021). What drives risk perceptions? Revisiting public perceptions of food hazards associated with production and consumption. *Journal of Risk Research*, 1–15. https://doi.org/10.1080/13669877.2020.1871057

Jenkins, S. C., Harris, A. J. L., Wandala, A., Ayuliana, S., Novikarany, R., Khalid, N. B. M., Mamat, C. S. N. B. C., Moron, L. A., Monteverde, M. C. A., Cayanan, E., & Beckett, R. (2022). Impact-based forecasting in South East Asia – what underlies impact perceptions? *International Journal of Disaster Risk Reduction*, *76*(June). https://doi.org/10.1016/j.ijdrr.2022.102943

Jenkins, S. C., Lachlan, R. F., & Osman, M. (2024). An integrative framework for mapping the psychological landscape of risk perception. *Scientific Reports*, *14*(1), 10989. https://doi.org/10.1038/s41598-024-59189-y

Klobas, J. E., McGill, T., & Wang, X. (2019). How perceived security risk affects intention to use smart home devices: A reasoned action explanation. *Computers & Security*, *87*, 101571.

Li, W., Yigitcanlar, T., Erol, I., & Liu, A. (2021). Motivations, barriers and risks of smart home adoption: From systematic literature review to conceptual framework. *Energy Research & Social Science*, *80*, 102211. https://doi.org/10.1016/j.erss.2021.102211

Nicholson, J., Skye Lukins, R., Coventry, L., Buil-Gil, D., Kuenzel, S., Blackwell, R., Zakhary, S., & Tilley, D. (2025). 'I need to be convinced that I need to become smart': Older adults views on consumer products with internet connectivity. *Journal of Risk Research*, *28*(2), 169–176. https://doi.org/10.1080/13669877.2025.2496232

OECD. (2019). *OECD Skills Outlook 2019: Thriving in a Digital World*. OECD Publishing. https://www.oecd.org/en/publications/oecd-skills-outlook-2019_df80bc12-en/full-report/component-7.html

Office for Product Safety & Standards. (2024). *Psychological factors underpinning risk perceptions*. https://www.gov.uk/government/publications/psychological-factors-underpinning-risk-perceptionsOliveira, L., Mitchell, V., & May, A. (2020). Smart home technology—comparing householder expectations at the point of installation with experiences 1 year later. *Personal and Ubiquitous Computing*, *24*(5), 613-626.

Osman, M. (2025a). Psychological harm: Implications for the scientific risk analysis and policy communities. *Journal of Risk Research*, *28*(2), 190–195. https://doi.org/10.1080/13669877.2025.2510923

Osman, M. (2025b). Psychological Harm: What is it and how does it apply to consumer products with internet connectivity? *Journal of Risk Research*, *28*(2), 1–22. https://doi.org/10.1080/13669877.2025.2491086

Posit Team. (2022). *RStudio: Integrated Development Environment for R* [Computer software]. Posit Software, PBC.

Product Security and Telecommunications Infrastructure Act 2022 (2022). https://www.legislation.gov.uk/ukpga/2022/46/contents

R Core Team. (2022). *R: A language and environment for statistical computing.* [Computer software]. https://www.r-project.org/

Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on General Product Safety, Amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and Repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC (Text with EEA Relevance), 135 OJ L (2023). http://data.europa.eu/eli/reg/2023/988/oj

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA Relevance) (2024). http://data.europa.eu/eli/reg/2024/2847/oj

Regulations on the Management of Security Vulnerabilities in Network Products (2021). https://www.gov.cn/zhengce/zhengceku/2021-07/14/content_5624965.htm

Renn, O. (1998). The role of risk perception for risk management. *Reliability engineering & system Safety*, *59*(1), 49-62.

Rijsdijk, S. A., & Hultink, E. J. (2003). 'Honey, have you seen our hamster?' Consumer evaluations of autonomous domestic products. *Journal of Product Innovation Management*, *20*(3), 204–216. https://doi.org/10.1111/1540-5885.2003003

Rijsdijk, S. A., & Hultink, E. J. (2009). How today's consumers perceive tomorrow's smart products. *Journal of Product Innovation Management*, *26*(1), 24–42. https://doi.org/10.1111/j.1540-5885.2009.00332.x

Ruohonen, J. (2022). A review of product safety regulations in the European Union. *International Cybersecurity Law Review*, *3*, 345–366. https://doi.org/10.1365/s43439-022-00057-8

Seymour, V., Xenitidou, M., Timotijevic, L., Hodgkins, C. E., Ratcliffe, E., Gatersleben, B., Gilbert, N., & Jones, C. R. (2024). Public acceptance of smart home technologies in the UK: a citizens' jury study. *Journal of decision systems*, 1-27.

Shank, D. B., Wright, D., Lulham, R., & Thurgood, C. (2021). Knowledge, perceived benefits, adoption, and use of smart home products. *International Journal of Human–Computer Interaction*, *37*(10), 922-937.

Skjott Linneberg, M., & Korsgaard, S. (2019). Coding qualitative data: A synthesis guiding the novice. *Qualitative Research Journal*, *19*(3), 259–270. https://doi.org/10.1108/QRJ-12-2018-0012

Statista. (2025). *Smart home device ownership in the UK as of June 2025* [Data set]. https://www-statista-com/forecasts/997845/smart-home-device-ownership-in-the-uk

Tabachnick, B. G., & Fidell, L. S. (2001). *Using Multivariate Statistics* (Fourth Edi). Allyn & Bacon.

Vaubel, K. P., & Young, S. L. (1992a). Components of perceived risk for consumer products. *Proceedings of the Human Factors Society*, *1*, 494–498. https://doi.org/10.1177/154193129203600505

Vaubel, K. P., & Young, S. L. (1992b). Components of Perceived Risk for Consumer Products. *Proceedings of the Human Factors Society Annual Meeting*, *36*(5), 494–498. https://doi.org/10.1177/154193129203600505

Wachinger, G., Renn, O., Begg, C., & Kuhlicke, C. (2013). The Risk Perception Paradox-Implications for Governance and Communication of Natural Hazards: The Risk Perception Paradox. *Risk Analysis*, *33*(6), 1049–1065. https://doi.org/10.1111/j.1539-6924.2012.01942.xWilson, C., Hargreaves, T., & Hauxwell-Baldwin, R. (2015). Smart homes and their users: a systematic analysis and key challenges. *Personal and Ubiquitous Computing*, *19*(2), 463-476.

Wilson, C., Hargreaves, T., & Hauxwell-Baldwin, R. (2017). Benefits and risks of smart home technologies. *Energy policy*, *103*, 72-83.

Wogalter, M. S., Desaulniers, D. R., & Brelsford, J. W. (1986). Perceptions of Consumer Products: Hazardousness and Warning Expectations. *Proceedings of the Human Factors Society Annual Meeting*, *30*(12), 1197–1201. https://doi.org/10.1177/154193128603001213

Wogalter, M. S., Desaulniers, D. R., & Brelsford, J. W. (1987). Consumer products: How are the hazards perceived? *Proceedings of the Human Factors Society Annual Meeting*, *31*(5), 615–619. https://doi.org/10.1177/154193128703100530

Young, S. L., & Laughery, K. R. (1994). Components of perceived risk: A reconciliation of previous findings. *Proceedings of the Human Factors and Ergonomics Society*, *2*(1992), 888–892. https://doi.org/10.1177/154193129403801420

Young, S. L., Wogalter, M. S., & Brelsford, J. W. (1992). Relative contribution of likelihood and severity of injury to risk perceptions. *Proceedings of the Human Factors Society*, *2*(1979), 1014–1018. https://doi.org/10.1177/154193129203601321

Zeelenberg, M., & Kogler, C. (2025). A note on psychological harm as a policy instrument. *Journal of Risk Research*, *28*(2), 161–164.

Zhu, Y., Bechlivanidis, C., & Osman, M. (2021). UK Government Report. Public Perceptions of CPIC: Attributions of Risk and Blame in Smart Product Failure. https://assets.publishing.service.gov.uk/media/61486d6a8fa8f503b680e998/public-perceptions-of-smart-products-summary-report.pdf

Supplementary Materials

Supplementary Materials 1

INSERT IMPORTANCE/PURSUIT GRAPHS.

Supplementary Materials 2

Table S1.

Products and Associated Descriptions.

Product	Description
Smart Pet Feeder	A device that automatically feeds pets food at regular intervals, often with metering and remote control options.
Smart Speaker	An audio device that connects to the Internet and features a voice assistant that can play music, answer questions, and control smart home devices through voice commands.
Teddy Camera	Smart surveillance cameras in the shape of teddy bears, capable of video recording, real-time monitoring and remote access.
Connected Children's Toy	A robot provides interactivity and educational features such as teaching language, maths, or programming skills, which is aimed at elementary school students (3-12 years old) age groups.
Smart Doorbell	A doorway-mounted device that provides real-time video surveillance, voice calls and remote access control via a mobile app or cloud connection.
Smart Toothbrush	An electric toothbrush equipped with sensors and connectivity to track brushing habits, provide real-time feedback and syncs with mobile apps.
Bluetooth Tracker	A small device that connects to a mobile phone via Bluetooth technology and is used to help locate and track the location of items.
Smart Door Lock	A door locking system equipped with electronic or wireless technology that allows for convenient and secure access control via password, fingerprint, mobile app or remote control.
Robot Sweeper	A robot that automatically cleans floors, using lasers, cameras or sensors to navigate and clean the floor.
Smart Watch	A smart wearable device, usually connected to a mobile phone, that provides functions such as time display, health monitoring, notification alerts and exercise tracking.

Supplementary Materials 3

Model Specification Process

(Risk Perceptions/Risk Tolerance): We specified a weakly informative prior ~ *N* (0,10) for all model parameters. This prior specification was used as no existing similar data existed. Four Markov chains were implemented for each parameter and the model was run for 8000 iterations with a burn-in phase of 1000 iterations. To assess convergence, the Gelman and Rubin (Gelman & Rubin, 1992) convergence diagnostic was implemented with the default setting, which indicated that convergence was achieved.

Supplementary Materials 4

Risk factors: Examining the relationships between the five risk ratings (equipment safety, psychological harm, data security, physical health, social relationships) on ratings of concern

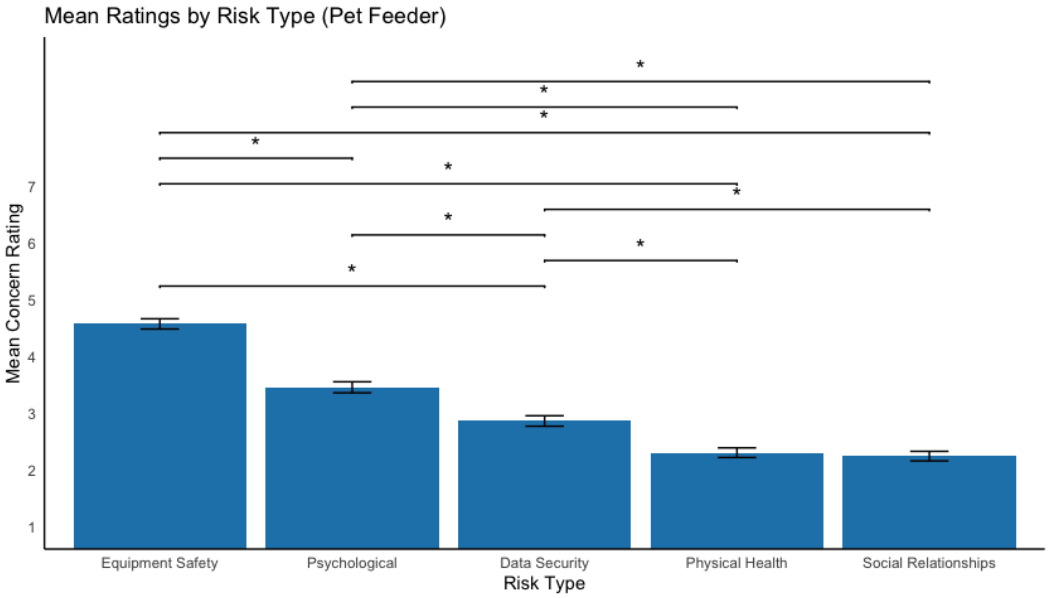
Pet Feeder

There was a significant effect of risk type on concern ratings, $F(4, 1985) = 115.2$, $p < .001$, $\eta^2 = 0.19$. Follow up Tukey HSD comparisons[3] demonstrated significant differences between concern ratings for all but one pair, see Figure 1.

Figure 1.

[3] All Tukey HSD comparisons were carried out with a Bonferroni correction applied, with significance depicted by * in the figures.

Mean Concern Ratings for Risk Type – Pet Feeder

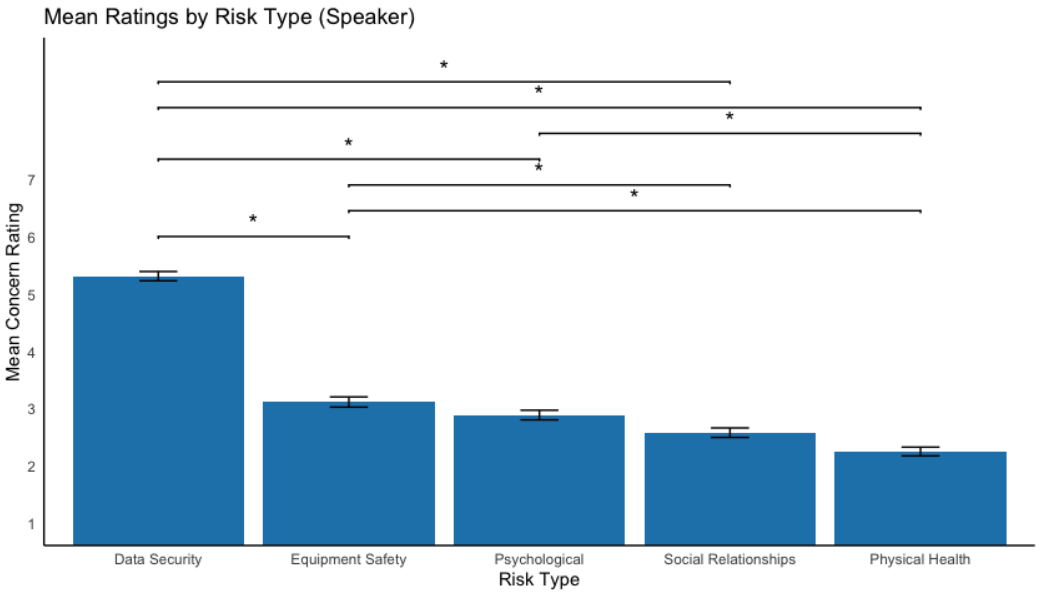


Speaker

There was a significant effect of risk type on concern ratings, $F(4, 1985) = 213.8$, $p < .001$, $\eta^2 = 0.30$. Follow up Tukey HSD tests demonstrated significant differences between concern ratings for seven comparisons (see Figure 2).

Figure 2.

Mean Concern Ratings for Risk Type – Speaker

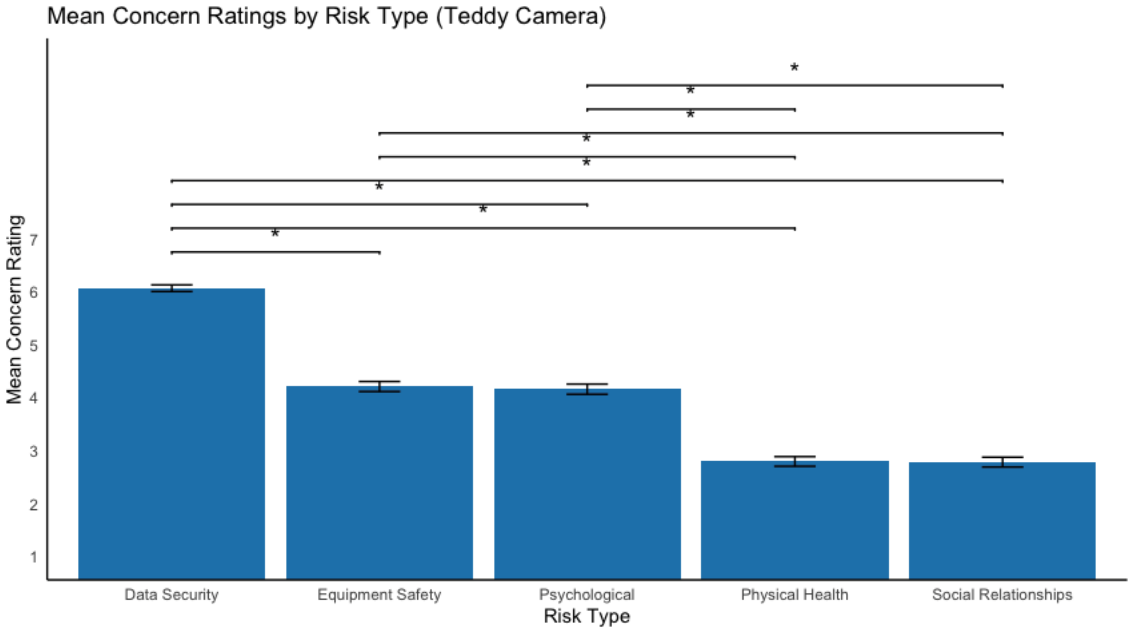


Teddy Camera

There was a significant effect of risk type on concern ratings, $F(4, 1985) = 232.6$, $p < .001$, $\eta^2 = 0.32$. Follow up Tukey HSD tests demonstrated significant differences between concern ratings for seven comparisons (see Figure 3).

Figure 3.

Mean Concern Ratings for Risk Type – Teddy Camera

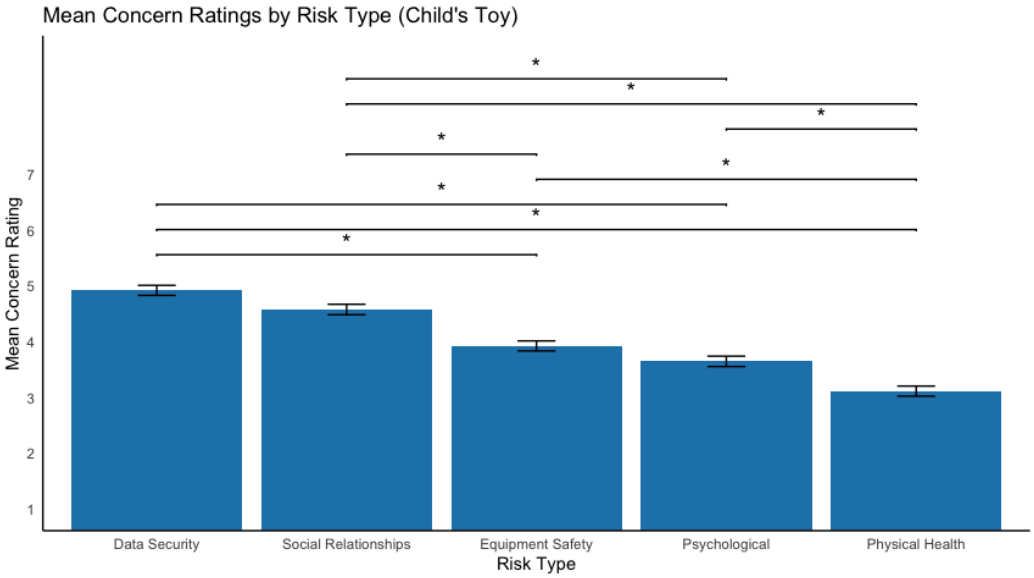


Child's Toy

There was a significant effect of risk type on concern ratings, $F(4, 1965) = 62.21$, $p < .001$, $\eta^2 = 0.11$. Follow up Tukey HSD tests demonstrated significant differences between concern ratings for eight pairwise comparisons (see Figure 4).

Figure 4.

Mean Concern Ratings for Risk Type – Child's Toy

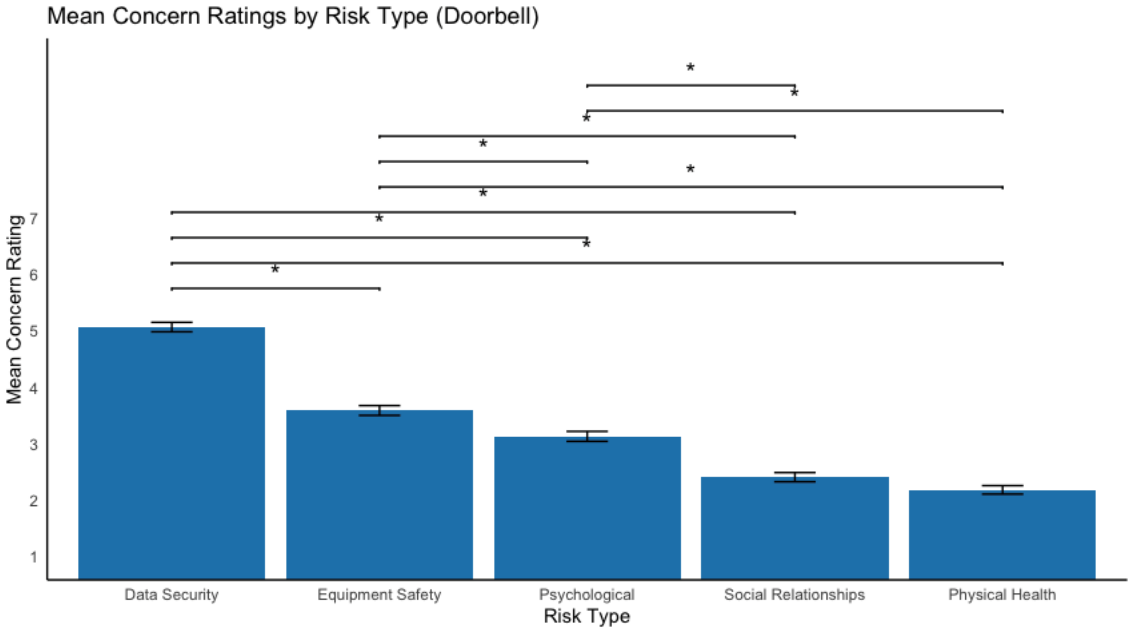


Doorbell

There was a significant effect of risk type on concern ratings, $F(4, 1954) = 190.0$, $p < .001$, $\eta^2 = 0.28$. Follow up Tukey HSD tests demonstrated significant differences between concern ratings for eight pairwise comparisons (see Figure 5).

Figure 5.

Mean Concern Ratings for Risk Type – Doorbell

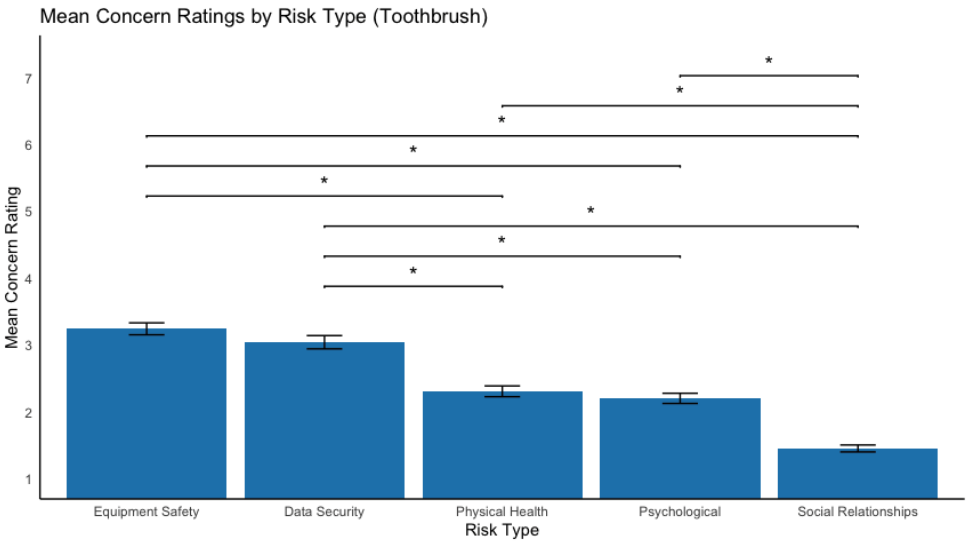


Toothbrush

There was a significant effect of risk type on concern ratings, $F(4, 1990) = 78.2$, $p < .001$, $\eta^2 = 0.14$. Follow up Tukey HSD tests demonstrated significant differences between concern ratings for eight pairwise comparisons (see Figure 6).

Figure 6.

Mean Concern Ratings for Risk Type – Toothbrush

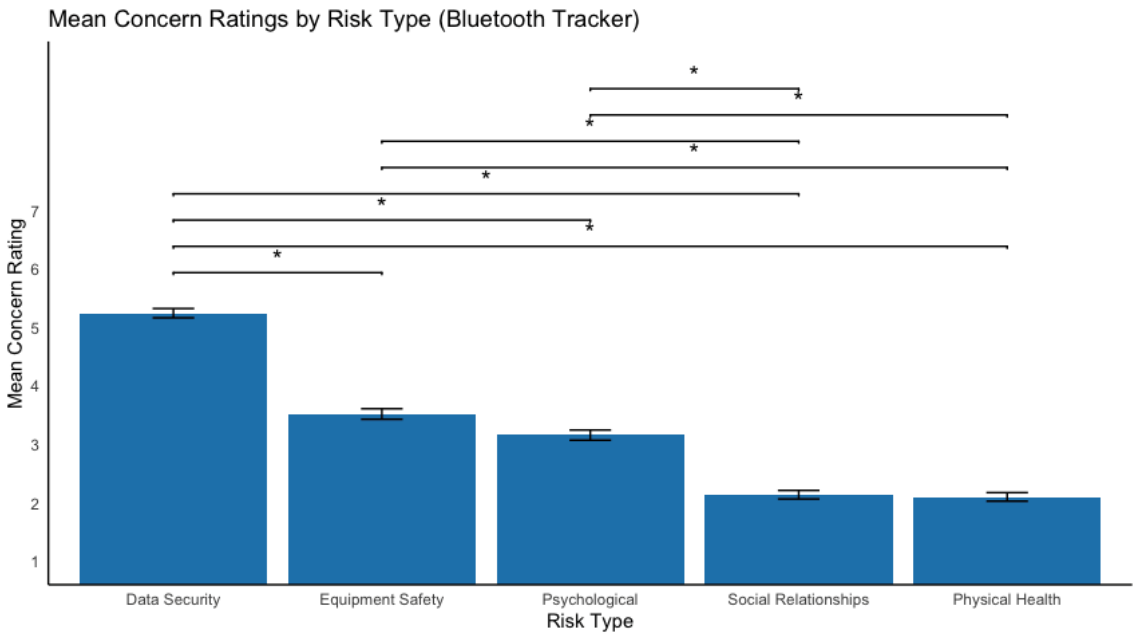


Bluetooth Tracker

There was a significant effect of risk type on concern ratings, $F(4, 1969) = 252.3$, $p < .001$, $\eta^2 = 0.34$. Follow up Tukey HSD tests demonstrated significant differences between concern ratings for eight pairwise comparisons (see Figure 7).

Figure 7.

Mean Concern Ratings for Risk Type – Bluetooth Tracker

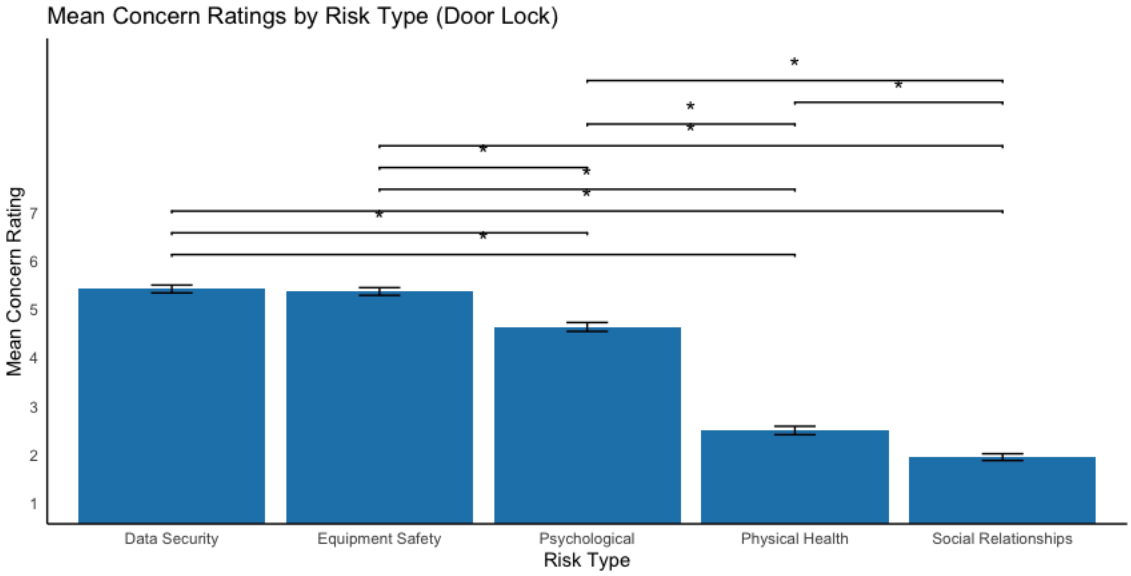


Door Lock

There was a significant effect of risk type on concern ratings, $F(4, 1949) = 397.9$, $p < .001$, $\eta^2 = 0.45$. Follow up Tukey HSD tests demonstrated significant differences between concern ratings for nine pairwise comparisons (see Figure 8).

Figure 8.

Mean Concern Ratings for Risk Type – Door Lock

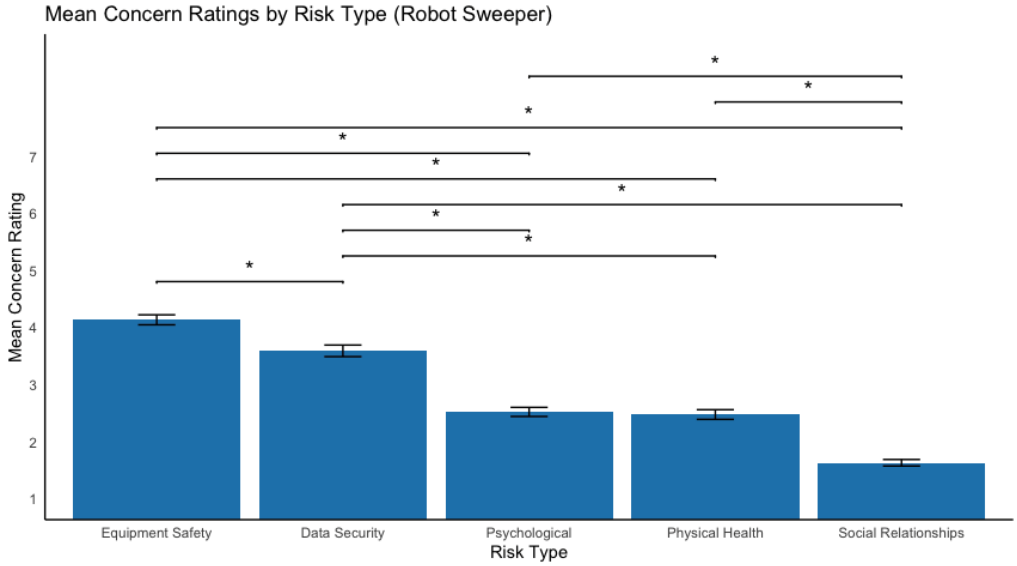


Robot Sweeper

There was a significant effect of risk type on concern ratings, $F(4, 1970) = 141.6$, $p < .001$, $\eta^2 = 0.22$. Follow up Tukey HSD tests demonstrated significant differences between concern ratings for nine pairwise comparisons (see Figure 9).

Figure 94.

Mean Concern Ratings for Risk Type – Robot Sweeper

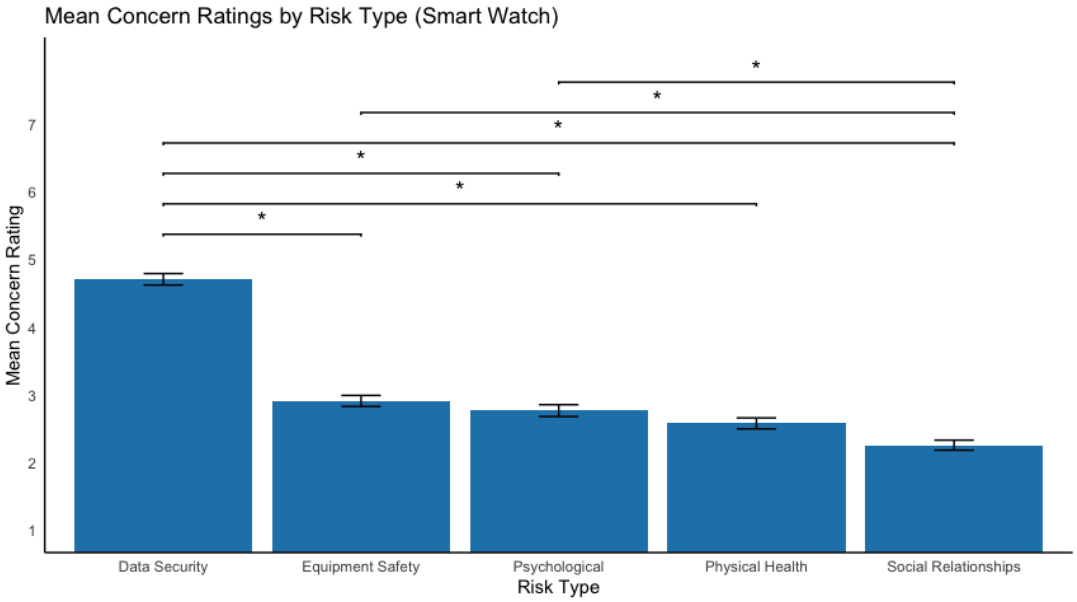


Smart Watch

There was a significant effect of risk type on concern ratings, $F(4, 1980) = 137.5$, $p < .001$, $\eta^2 = 0.22$. Follow up Tukey HSD tests demonstrated significant differences between concern ratings for six pairwise comparisons (see **Error! Reference source not found.**0).

Figure 10.

Mean Concern Ratings for Risk Type – Smart Watch



Supplementary Materials 5

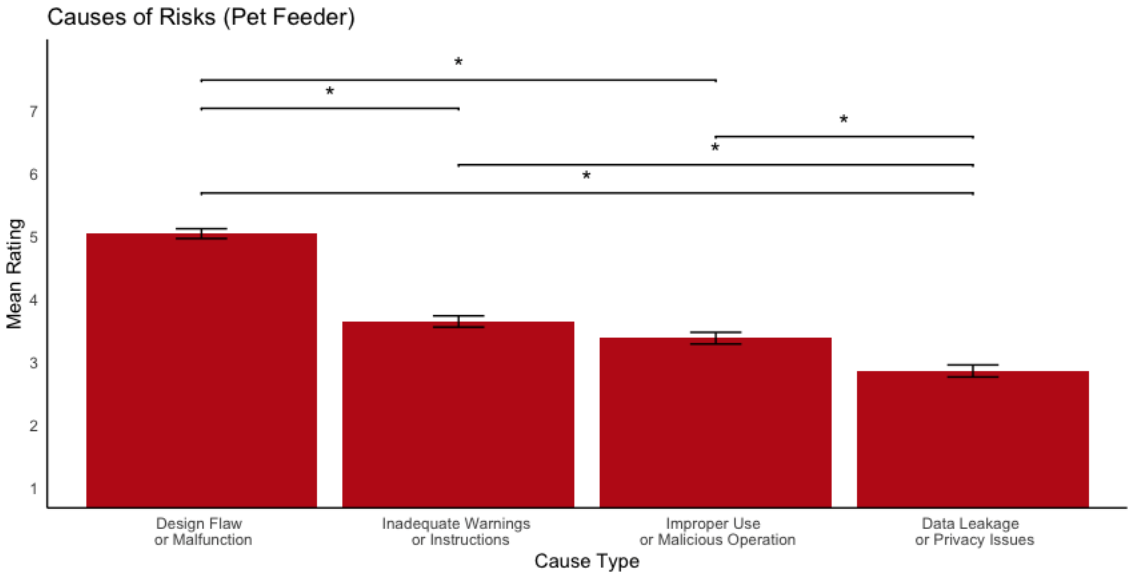
Causal factors: Examining the relationships between the five risk ratings (equipment safety, psychological harm, data security, physical health, social relationships) on ratings of concern

Pet Feeder

There was a significant effect of cause type on ratings of concern, $F(3, 1588) = 109.0$, $p < .001$, $\eta^2 = 0.17$. Follow up Tukey HSD comparisons[4] demonstrated significant differences between five pairs of ratings (see Figure 11).

Figure 11.

Mean Ratings for Cause Type – Pet Feeder



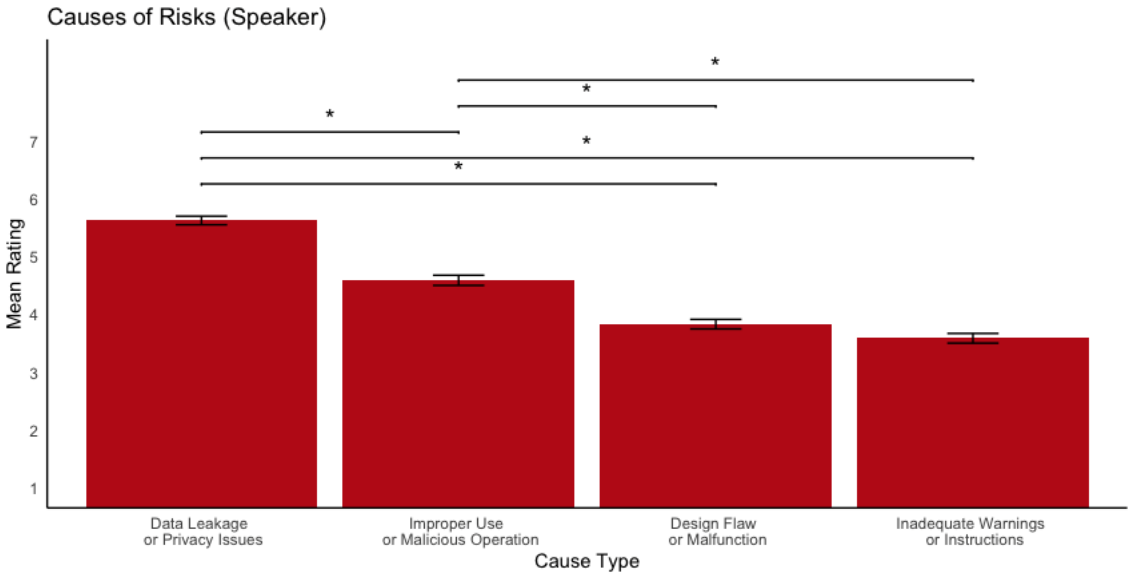
[4] All Tukey HSD comparisons were carried out with Bonferroni correction applied.

Speaker

There was a significant effect of cause type on ratings of concern, $F(3, 1580) = 123.8$, $p < .001$, $\eta^2 = 0.19$. Follow up Tukey HSD comparisons demonstrated significant differences between five pairs of ratings, see Figure 12.

Figure 12.

Mean Ratings for Cause Type – Speaker

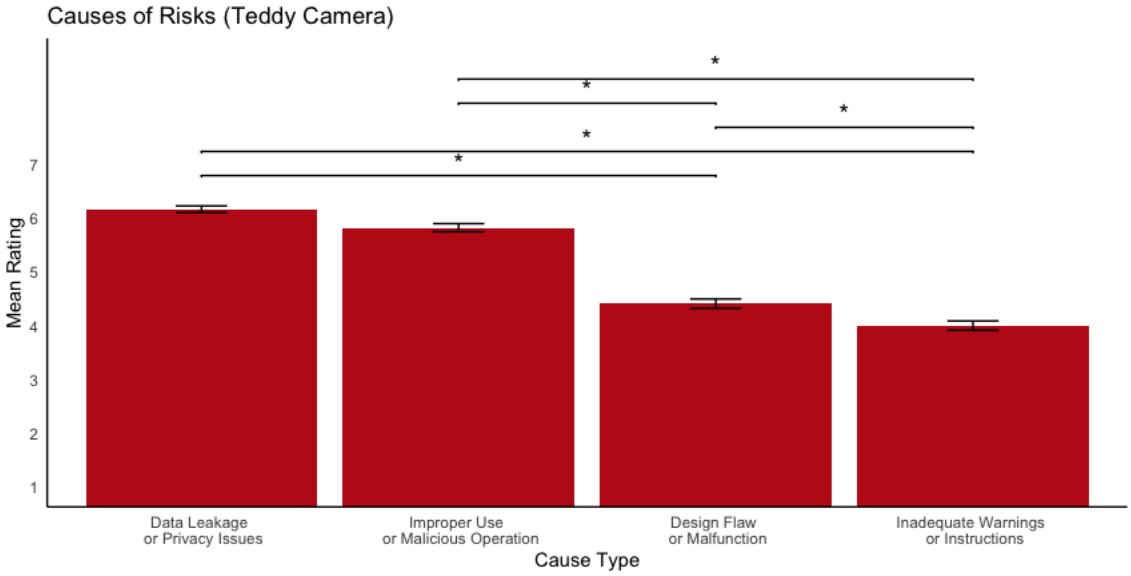


Teddy Camera

There was a significant effect of cause type on ratings of concern, $F(3, 1588) = 184.1$, $p < .001$, $\eta^2 = 0.26$. Follow up Tukey HSD comparisons demonstrated significant differences between five pairs of ratings, see Figure 13.

Figure 13.

Mean Ratings for Cause Type – Teddy Camera

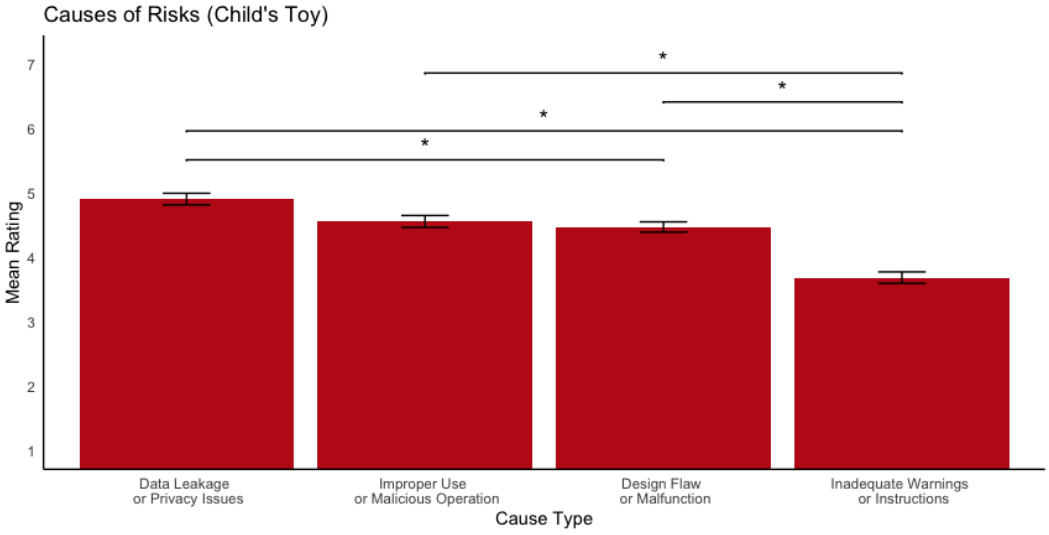


Child's Toy

There was a significant effect of cause type on ratings of concern, $F(3, 1572) = 34.44$, $p < .001$, $\eta^2 = 0.06$. Follow up Tukey HSD comparisons demonstrated significant differences between four pairs of ratings, see Figure 14.

Figure 14.

Mean Ratings for Cause Type – Child's Toy

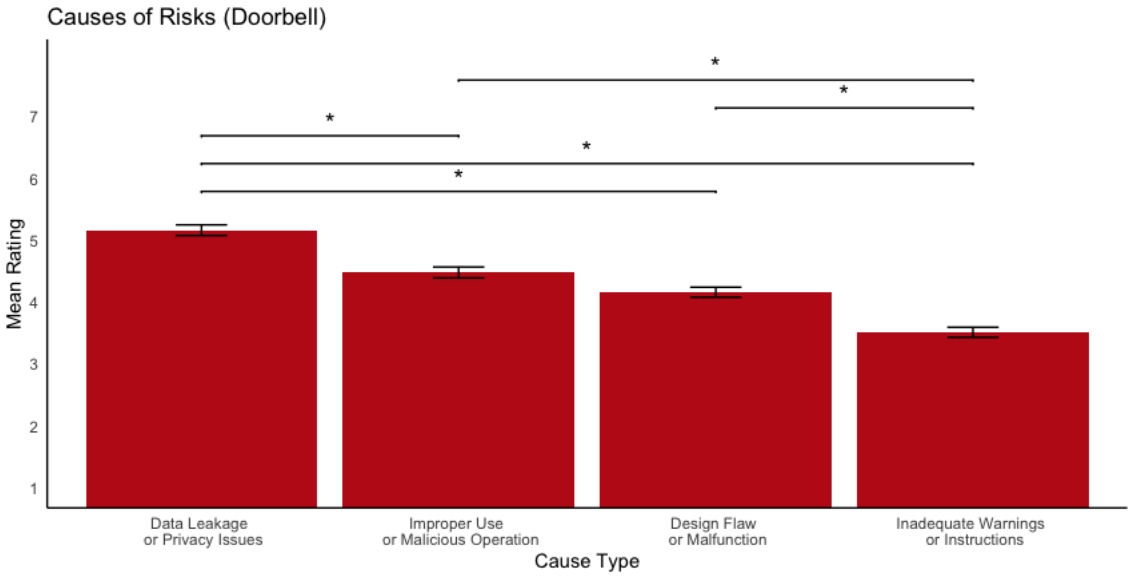


Doorbell

There was a significant effect of cause type on ratings of concern, $F(3, 1564) = 66.05$, $p < .001$, $\eta^2 = 0.11$. Follow up Tukey HSD comparisons demonstrated significant differences between five pairs of ratings, see Figure 15.

Figure 15.

Mean Ratings for Cause Type – Doorbell

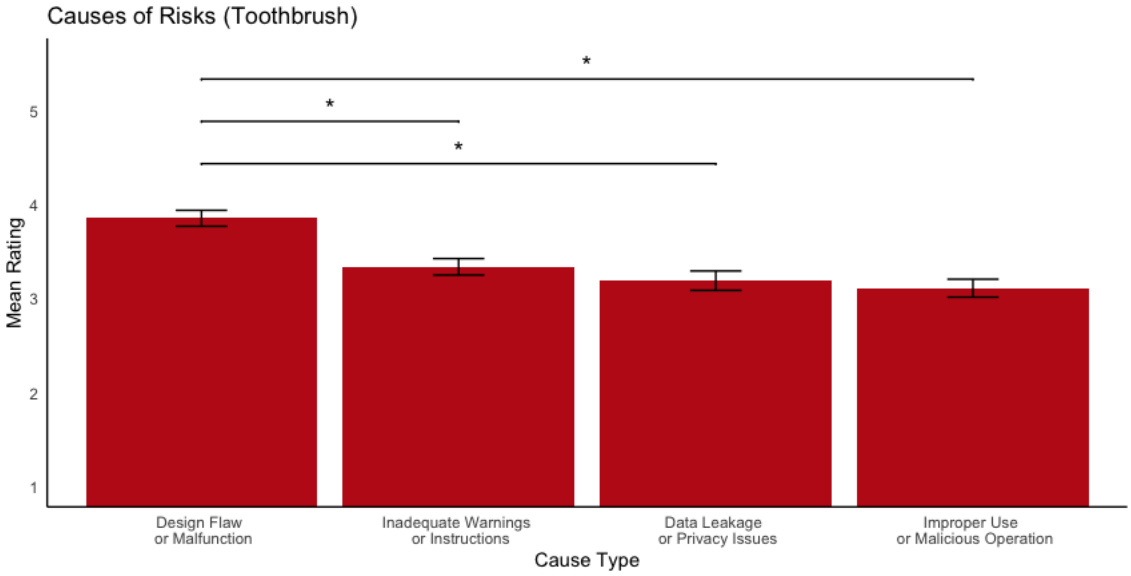


Toothbrush

There was a significant effect of cause type on ratings of concern, $F(3, 1591) = 12.88$, $p < .001$, $\eta^2 = 0.02$. Follow up Tukey HSD comparisons demonstrated significant differences between three pairs of ratings, see Figure 16.

Figure 16.

Mean Ratings for Cause Type – Toothbrush

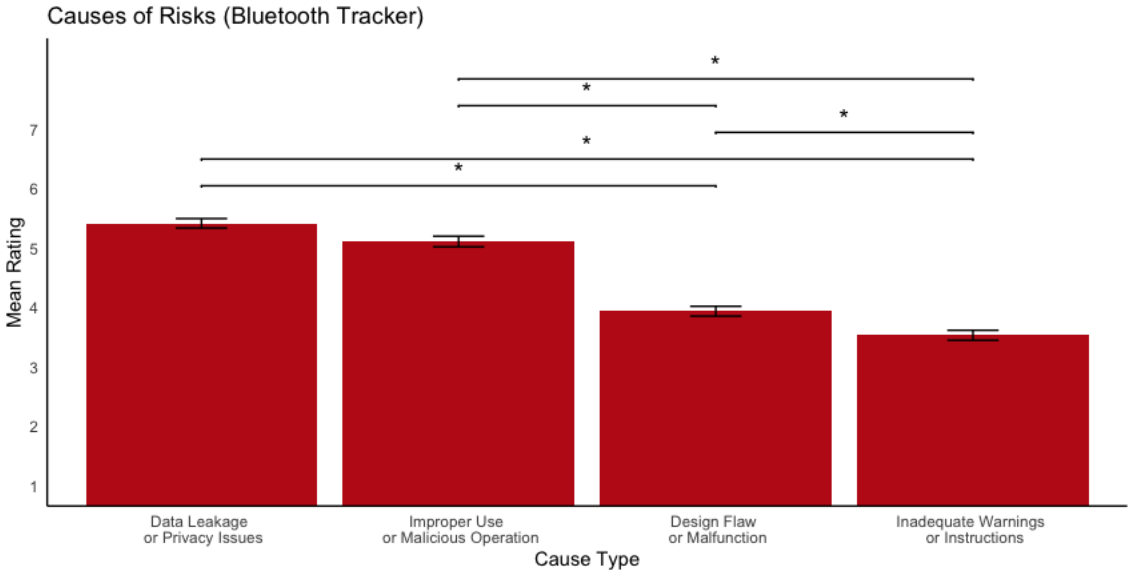


Bluetooth Tracker

There was a significant effect of cause type on ratings of concern, $F(3, 1576) = 116.6$, $p < .001$, $\eta^2 = 0.18$. Follow up Tukey HSD comparisons demonstrated significant differences between five pairs of ratings, see Figure 17.

Figure 17.

Mean Ratings for Cause Type – Bluetooth Tracker

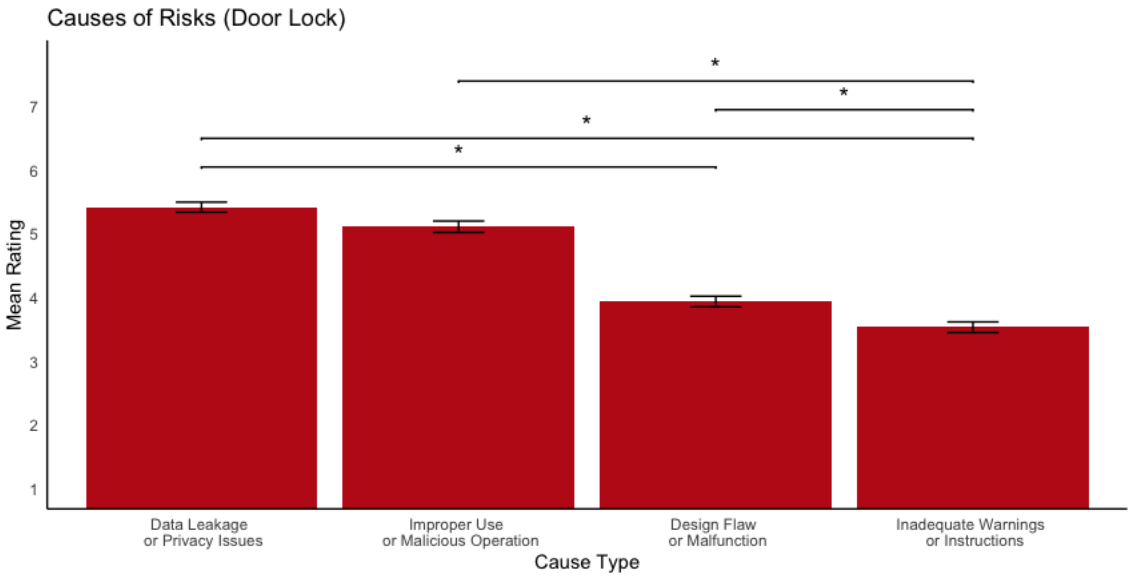


Door Lock

There was a significant effect of cause type on ratings of concern, $F(3, 1560) = 37.41$, $p < .001$, $\eta^2 = 0.07$. Follow up Tukey HSD comparisons demonstrated significant differences between four pairs of ratings, see Figure 18.

Figure 18.

Mean Ratings for Cause Type – Door Lock

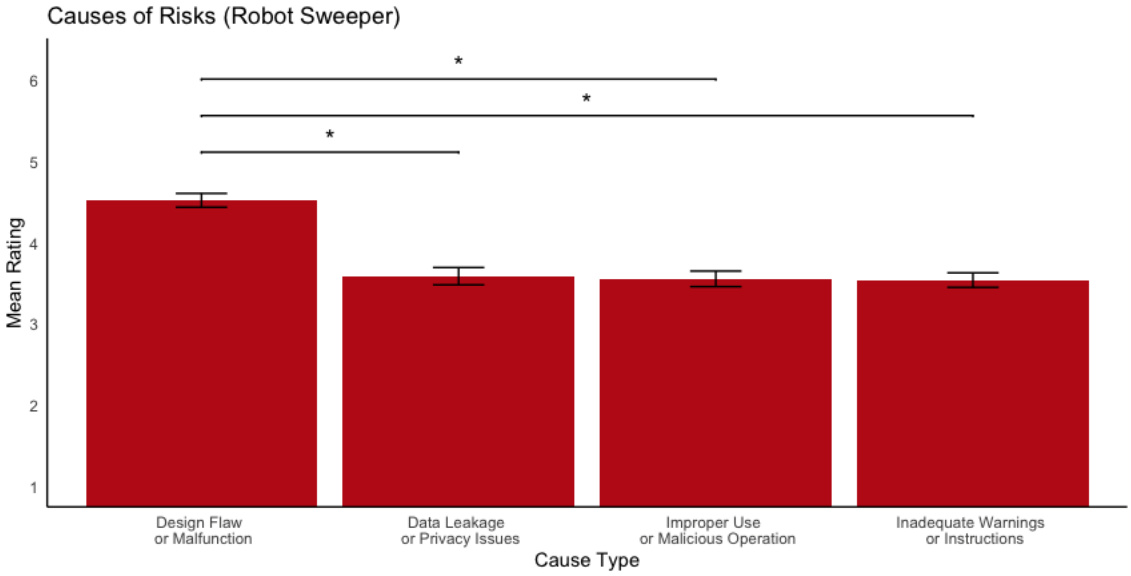


Robot Sweeper

There was a significant effect of cause type on ratings of concern, $F(3, 1576) = 25.87$, $p < .001$, $\eta^2 = 0.05$. Follow up Tukey HSD comparisons demonstrated significant differences between three pairs of ratings, see Figure 19.

Figure 19.

Mean Ratings for Cause Type – Robot Sweeper



Smart Watch

There was a significant effect of cause type on ratings of concern, $F(3, 1584) = 75.36$, $p < .001$, $\eta^2 = 0.12$. Follow up Tukey HSD comparisons demonstrated significant differences between four pairs of ratings, see Figure 10.

Figure 20.

Mean Ratings for Cause Type – Smart Watch