USENIX

THE ADVANCED COMPUTING
SYSTEMS ASSOCIATION

Regulating Smart Device Support Periods: User Expectations and the European Cyber Resilience Act

Lorenz Kustosch and Carlos Gañán, *Delft University of Technology;*
Mattis van 't Schip, *Radboud University;* Michel van Eeten and
Simon Parkin, *Delft University of Technology*

https://www.usenix.org/conference/usenixsecurity25/presentation/kustosch-regulating

This paper is included in the Proceedings of the
34th USENIX Security Symposium.

August 13–15, 2025 • Seattle, WA, USA

978-1-939133-52-6

Open access to the Proceedings of the
34th USENIX Security Symposium is sponsored by USENIX.

Regulating Smart Device Support Periods: User Expectations and the European Cyber Resilience Act

Lorenz Kustosch
Delft University of Technology

Carlos Gañán
Delft University of Technology

Mattis van 't Schip
Radboud University

Michel van Eeten
Delft University of Technology

Simon Parkin
Delft University of Technology

Abstract

Supporting consumer IoT devices with updates is crucial to ensure their security. However, this support period is usually shorter than the device's actual lifespan, resulting in millions of unsupported and vulnerable devices. The upcoming European Cyber Resilience Act (CRA) addresses this by requiring manufacturers to support their products for the expected use time, which should be based on reasonable user expectations. In this work, we thus empirically explore the concept of user expectations regarding smart devices' use times and security provisions by conducting a large-scale survey in five EU countries (n = 993). We find that respondents' smart device use times and lifetime expectations exceed the CRA's baseline of five years for a majority of device categories and vary substantially across device categories, their "smartness", and individuals. Respondents also consider different factors for the lifetimes of smart and conventional devices. Surprisingly, a majority of respondents expected update support to correspond with devices' full lifetimes, highlighting how the current market dynamics of short support times seem to contrast expectations. Our results provide novel insights for manufacturers and market authorities who will need to determine support periods for smart products in the coming years.

1 Introduction

To secure the growing population of consumer IoT devices from an evolving threat landscape, continuous support over the product's lifecycle is crucial. However, security updates for such smart devices often end prematurely and their presence or duration is often not disclosed to consumers at purchase. A recent report from the US Federal Trade Commission found that for 89% of the reviewed smart products, no disclosure on the duration of updates support was provided [18], seemingly a status-quo in the smart device market [39, 42].

Various regulatory and policy initiatives aim to increase transparency of the software support duration to provide certainty to consumers about the security capabilities of the devices that they purchase. Within this, there is an expectation that consumers will gravitate toward more secure devices within purchase decisions. The US Cyber Trust Mark announced in 2023 is a voluntary product labeling scheme where manufacturers of smart devices disclose the support period as part of the label [17, 31]. In the UK, the PSTI act *requires* manufacturers to disclose a minimum support period for security updates [46] to comply with the law, instead of the voluntary label approach in the US.

While *disclosing* information to consumers for a more informed purchase is an important step, the question then arises of *how long* this support should actually be provided. The approach of the European Commission is embodied in the Cyber Resilience Act (CRA) [49], launched in 2024 and coming into force in 2027; to the best of our knowledge, the CRA is the first regulation that explicitly sets legal product requirements on a *duration* for how long security measures must be provided across a broad range of products.Specifically, security vulnerabilities of "products with digital elements" must receive security updates for their *expected use time* but at least five years[1].

In the determination of the expected use time, that is, device lifetime, reasonable user expectations play a crucial role. Manufacturers will have to actively determine this period based on users' expectations and disclose how they considered this in the product's technical documentation. Similarly, market surveillance authorities will check such documentation and, in turn, determine what they see as a reasonable user expectation to determine compliance with the CRA. If they find that the support duration for a product violates expectations, they could remove the device from the EU market.

Thus, the user perspective, previously an afterthought in security support duration, suddenly takes center stage in the regulatory realm with global implications. Manufacturers sell the same smart devices in other markets than the EU and could streamline global compliance efforts and release the same security updates as in the EU, following the "Brussels

[1] With exceptions possible (Article 13.8. and Recital 60).

Effect" [7,30,37]. However, the abstract concept of reasonable user or consumer expectations regarding a product's expected use time bears uncertainty for smart device manufacturers and market surveillance authorities. For instance, is it reasonable to expect that a smart washing machine will be used for longer than a smartwatch and should thus be patched for longer?

Prior research only provides limited insights into the use time or update support duration of smart devices. While [23] studied smart home users' perspectives on the end of support and [28] empirically measured reasonable consumer expectations regarding security and privacy incidents with consumer IoT devices, the expected or observed *duration* of device use or update support has not been directly measured, although [33,35] find that longer support periods were generally preferred by consumers.

As the CRA explicitly links the duration for security support to users' expectations of the product's lifetime, we aim to fill this gap by conducting a large survey among EU consumers to empirically assess their expectations and behaviors regarding smart device use times. We ask the following Research Questions: (i) How do consumers use their smart devices, and for how long?; (ii) How long do consumers expect different smart device categories to last, and which factors influence these expectations?, (iii) How do consumers perceive security and software update support over smart devices' lifespans?, and; (iv) Are there differences among EU member states regarding consumers' smart device usage, expectations, and security and software support perceptions?

We make the following contributions:

- We conduct an online survey with 993 participants in five different EU member states and collect empirical data on and explain a methodological approach to a concept of high relevance in the coming years: Smart device use times and users' expectations regarding them. Thus, we provide an empirical basis for manufacturers and market surveillance authorities how to conceptualize and approach users' expectations regarding smart product lifetimes.
- We measure smart device *use times* by studying 2753 individual smart devices and measure lifetime *expectations* via smart device vignettes. While expectations varied across devices and individuals, we find that, in aggregation, almost all studied smart products were expected to last longer than the CRA's baseline of five years, despite respondents factoring in aspects like fast innovation and replacement, incompatibility, or planned obsolescence. Additionally, a majority of respondents expected update support to correspond to the device's full lifetime, highlighting how the CRA's provisions seem to meet expectations already.
- We extend previous work on smart devices' end of support by focusing on the concept of security support *duration*. We find that respondents were aware of security updates being crucial to mitigate security risks, although updates were generally opaque (non-perceptible), and their eventual end was not a strong trigger to stop device usage - better alternatives or declining functional performance were much stronger motivators.

In the remainder of the paper, we first consider the regulatory underpinnings and related work on users' expectations regarding smart devices, followed by our survey methodology and results. We then contextualize our findings in the wider regulatory and academic field and provide recommendations for manufactures and market authorities.

2 Background and Related Work

Here we frame existing IoT users' experiences with IoT security and privacy against legal processes involving reasonable expectations. These are then considered alongside the expectations then placed upon other actors in the market, such as manufacturers and retailers.

2.1 EU support duration regulations

User or "consumer" expectations are often part of legal considerations. In the context of cybersecurity, the most prominent piece of current legislation in the EU is the Cyber Resilience Act (CRA), adopted at the end of 2024. It regulates manufacturers that place "products with digital elements" (i.e., software and hardware products) on the EU market. It thus has global impact, as any manufacturer must adopt its measures when placing products on the EU market, regardless of their location. Internet of Things (IoT) devices are prominent examples of products with digital elements; they must adhere to numerous cybersecurity requirements (e.g., security-by-default, (Annex I(2)(a)). The CRA reserves a special position for certain categories of IoT devices. For instance, smart home security devices and virtual assistants are an "important" category due to larger security risks than average products with digital elements.

The manufacturer must, as part of a comprehensive list of requirements, ensure that any detected vulnerabilities are swiftly mitigated for the entire "support period" of their device. Manufacturers must determine this support period themselves, based on several criteria provided in the CRA (Article 13(8)). The manufacturers *shall* (i.e., must) consider in this determination: "reasonable user expectations", the nature of the product (including its intended purpose), and other EU legislation that may already determine lifetimes for the product category. Additionally, manufacturers *may* take into account support periods of similar products, the availability of operating environments, the support period for integral components of the product created by third-parties and guidance provided by administrative authorities (the "ADCO"). Manufacturers are thus obligated to take into account how long users would

reasonably expect their product to remain in use, i.e., the product's expected lifetime.

Manufacturers must include the chosen support period with the product's documentation (Article 13(19)). Furthermore, they must share the information on which they base the chosen support period (Article 13(8)). Market authorities must monitor chosen support periods and take corrective action when they consider the support period incorrect.

European product legislation often connects product support periods and user expectations. For instance, the Sale of Goods Directive (SG Directive) offers another example of this approach [48], aiming to protect consumers when signing a sales contract. It requires that goods with digital elements (e.g., smart products) remain in conformity with the sales agreement. For instance, a video app on a smart TV cannot suddenly lower its picture quality, if the initial contract noted a higher quality. It thus requires the product to receive updates, including security updates, "for the period of time [...] that the consumer may reasonably expect" to conform with the contract (Article 7(3)). However, in contrast to the CRA, the SG Directive does not place a burden on the seller to provide how they assessed their support period and to share it with consumers and market authorities.

Thus, the support period determined by the manufacturer plays a key role for smart devices in the EU. Manufacturers and market authorities must know what support periods are reasonable for a breadth of product categories. Consumers, at the same time, can compare support periods so they can make informed purchase decisions. Given these dynamics introduced by the CRA, it is vital to understand user expectations regarding support periods of products with digital elements.

2.2 Consumer expectations and perspectives of IoT security and product lifespans

Prior work has studied consumer expectations of security support for IoT devices [28] – this included manufacturer liability and responses in case of particular incidents, finding that expectations differ per device and that, when measuring expectations in the legal context, it is important to distinguish between reasonable (realistic) and normative expectations (ideal). Here we study conformity to update support commitments, as in the CRA.

Concerning software support for IoT specifically, there is great uncertainty among users, even when directly presented with pertinent information (such as "security labels") [22, 23], for instance that users say updates are important, but do not understand the implications of using unsupported devices or what end of support means [14], all the while lacking clarity as to the purpose of updates [24]. These outcomes point to users needing assurance in a market that is full of uncertainty – this suggests there could be value in not only setting a support duration, but strengthening assurances that it will remain over time, as a reliable "minimum" duration.

Further, when software support duration is considered as a product label attribute during device selection [15], prior work suggests there is a demand among consumers for the delivery of security updates for IoT devices for a longer period of time than they are accustomed to (e.g., [33, 35]). Thus, where previous work has suggested that support assurances would be valued, it lacks a clear connection to the expected duration of update support and, most importantly in the context of the CRA, the *expected* lifetime of IoT products, as [33, 35] measured *preferred* update support duration with predetermined values by the researchers (e.g., 2 years, 6 years, and lifetime).

However, consumers' expectations of products' lifetimes have been measured before, just not in the context of security and privacy, but in the domain of sustainability [12, 19, 20, 36, 38, 51]. For instance, [12, 19] and [38] measure expected lifetime or perceived longevity importance for product categories like mobile phones or vacuum cleaners. However, smart devices and the role of software updates and security were not directly studied. This research highlights different forms of product lifetime expectations, namely *intended* lifetime (how long a product is intended to be in use by its current owner), *ideal* lifetime (how long a product should ideally last), and *predicted* lifetime (how long a product will likely last). A conceptual piece by Bradley et al. examines similar concerns [8], outlining the conflicting interests between continued security patching and device longevity, proposing a paradigm shift: an architecture and differential responsibilities for different actors to keep devices running and secure for as long as possible. Here, we examine how user perceptions inform the provisions needed in determining support duration relative to the CRA.

In examining the electronics repair industry, Ceci et al. [10] found that 12% of their 112 survey participants stated that a smartphone or tablet never broke; however, the cost and hassle of getting a device repaired were major factors where participants had a device that developed problems but that they did not seek to get repaired. In studying views on IoT device obsolescence, Vats et al. [50] found that when interview participants were faced with external events such as an IoT device ceasing to function, needing an update, or losing smart features, they would try to find terms in the user agreement that would force the manufacturer to take responsibility (and feel a lack of agency if they could not); this indicates an existing gap that CRA assurances could fill. The interview participants of Haney et al. [21] referred to an unspoken agreement at device purchase, that a manufacturer should protect buyer security and privacy, but that participants differed in how sure they were that a manufacturer could uphold those expectations, trusting larger firms as being more competent to do so.

3 Method

To explore user expectations regarding smart devices' lifetimes, we conducted an online survey with 993 participants

recruited on the crowdsourcing platform Prolific [40] during November and December 2024. As the CRA is an EU legislation, we recruited an EU-based sample from France, Germany, Poland, Spain, and The Netherlands. We selected this subset as countries belong to the largest member states, together account for over half of the full EU population, vary in geographic location, culture, and markets, and to retain an appropriate sample size per country for robust statistical comparison. Due to the CRA requiring an EU-wide uniform approach, we were interested to study the potential variety of market dynamics across countries, such as user journeys, purchase channels, and experiences with smart devices and their security, potentially requiring differentiated support structures for users.

In the following, we detail our survey design, data collection and analysis, and the resulting sample.

3.1 Survey Design

We first explain some of our conceptual considerations around the notions of consumer expectations and device lifetime, followed by survey design and preparation for publication in different countries.

3.1.1 Conceptualizing device lifetime expectations

We aimed to align with the CRA definition of product lifetime, which is "the length of time during which the product is expected to be in use", which should be based on "reasonable user expectations, the nature of the product, including its intended purpose". Previous empirical work on consumer expectations provided a solid methodological basis for phrasing this question in a survey. Gnanapragasam et al. [20] stress the importance of clearly differentiating between three forms of expected product lifetimes: *Intended* (how long a product is intended to be in use by its current owner), *ideal* (how long a product should ideally last), and *predicted* (how long a product will likely last). Other related work on smart devices' consumer expectations highlights the necessity to differentiate *normative* (ideal) and *reasonable* (realistic) expectations and argues that realistic expectations correspond more closely to the legal notion of reasonableness, rather than normative ideals [28].

Thus, we conceptualized user expectations about product lifetimes according to the following two criteria:

- The expectation is about a *predicted* period of time for how long a given smart device will remain functional to be used for its intended purpose, not what is desired for how long it *ideally* should last. i.e., the expectation should be reasonable.
- This period should be independent of ownership, as devices can be sold or gifted onward [29], and we did not want to measure the initial use cycle, i.e., a user's preference when to move to a newer device.

Thus, when asking about the expected lifetime of a smart device, our question was: "*If you had to predict, for how many years do you expect such a device to last?*" (Q5.1.1). However, we also considered *intended* product lifetimes (how long a product is intended to be in use by its current owner) by inquiring with participants about how long they plan to continue using their *own* smart devices to then form a measure of their use time, adding up the durations of past use and intended future use.

3.1.2 Measuring device lifetime expectations

To quantify expectations about smart devices' lifespans, we designed vignettes for several prototypical devices and presented survey participants with a random subset of them to measure how long they would expect the device to last. Table 1 depicts our selection of devices and vignettes can be found in the survey instrument online[2].

Vignettes are short descriptions or scenarios, to provide respondents with context to elicit a response and are commonly used in security and privacy research [2, 3, 5, 28, 34]. Our vignettes described the device at hand, its high-level features, how it can be used, and its smart capabilities to ensure that respondents without any experience with it could also form a picture of this product. We followed common practice in security user research [23, 24, 28, 33], and selected a diverse range of smart devices with varying use cases, price points, and security and privacy implications and perceptions, which should all fall under the CRA.

As many white goods products become increasingly smart, we also tested whether expected lifetimes would differ between smart and conventional versions. We were interested in how participants would factor in the additional aspects introduced by the "smartness" into their expectations, such as software updates, online connectivity, and security or privacy risks.

We did not include a conventional version for all smart devices, as for some, we considered them an entirely different product based on their primary use case. For instance, we did not consider a regular watch (primary use: showing the time) a fair comparison to a smartwatch (primary use: running applications like health tracking, or messaging/notification).

3.1.3 Survey design process

We drafted the initial survey based on our research questions and the content examined for the literature review (Section 2). We also gathered feedback during a workshop with thirteen experts working in the fields of IoT security and law where the survey draft was presented, jointly discussed in the group, and subsequently improved regarding clarity, wording, and specificity of the IoT devices.

[2] https://doi.org/10.4121/71c038e7-e991-4dcd-9729-47dd0d9250c6

Device type	Product category	Conv. Comp.
Smart speaker	Entertainment	No
Smart thermostat	Home / Energy management	Yes
WiFi Solar inverter	Home / Energy management	Yes
Smart camera	Home security	No
Smart doorlock	Home security	No
Home router	Network equipment	No
Connected printer	Office equipment	Yes
Smart Smoke Detector	Sensors	Yes
Smart watch	Wearables	No
Smart washing machine	White Goods	Yes
Robot vacuum	White Goods	Yes

Table 1: Selection of devices used in the vignettes. "*Conv. Comp.*" denotes if a comparison to the conventional version of that product was made.

At this point, we involved policymakers and conducted four online meetings with policymakers from different EU member states, all involved in the drafting or future enforcement of the CRA. In the meetings, we inquired about their interpretations of the CRA's support period provisions and asked for their involvement in the study. We received feedback on our survey and suggestions for questions relevant to their work from 3 of the 4 organizations and then improved the survey regarding wording and flow and added a question about the purchase channels of respondents' own devices (Q2.4 & Q2.5), as this was of interest for several policymakers.

A pilot run of the survey was conducted with 25 participants recruited on Prolific to check for any technical problems, question understanding, completion time, or any answer options not provided in our multiple-choice questions (i.e., Q4.3, Q4.4, Q7, Q9.1, Q9.2). Participants took 14.8 minutes on average and no technical issues emerged. Only minor adjustments were necessary for some questions for clarity, despite the pilot survey allowing respondents to indicate where they felt unsure about their answer.

After the pilot study, the survey was translated from English into the five countries' respective languages (French, German, Polish, Spanish, and Dutch), by first being translated using Qualtrics' native automatic translation tool based on Google Translate [41]. This automatic translation was then checked and adjusted by five different native speakers (where this included names of popular online stores).

3.2 Recruitment and participants

Participants were recruited on the crowd-sourcing platform Prolific with the following screening criteria: Participants should reside in one of the five member states, be fluent in the respective official language, have an approval rate in prior studies of at least 95%, and completed at least five other submissions on the platform. We opened a separate survey invite for each age group to avoid bias towards younger cohorts, as Prolific samples tend to be younger [44]. In each age group, we also applied a quota for gender to get an even split. For the highest age brackets, we were not able to attain the full target sample size or an even gender split in all countries, as the number of available participants on Prolific for this target group was too small. We redistributed the remaining slots across the different age groups. The final sample consisted of 993 respondents and Table 2 depicts the demographic information.

We decided against screening for smart device ownership, given that the expectations of consumers without smart devices have legal relevance – they might be future users, or have their own particular reasons for not engaging with such products. Thus, we were able to compare expectations and perspectives between experienced and less experienced users of smart devices. We followed methodological literature for comparable experimental designs (i.e., factorial designs and choice experiments) to find sample sizes with sufficient statistical power for our planned device and country comparisons. [4] and [6] suggest a range of at least 5 to 50 observations per vignette as a general guideline for such designs with repeated measures (vignettes) per respondent and deploying multi-level regression for analysis. As we wanted to compare lifetime expectations of a total of 17 different device vignettes within each of the five countries, we aimed at 200 participants per country, as this would provide 35.3 responses on average per device per country, well above the minimum recommendation of five observations.

During data collection, we noticed that many respondents interpreted the survey questions about their own devices (Q2.1 - Q2.8) differently as intended by us, i.e., as asking about the general device category, not the particular device they were using right now (i.e., asking when they started using smartphones *in general*, instead of when they started their *currently used* smartphone). We thus added a clarification to Q2.2 to focus responses on the currently used devices, changed the wording of Q2.2 to Q2.8 accordingly, and then did a follow-up survey only with these specific questions with all respondents participating so far. We contacted them directly via Prolific and paid a higher hourly rate to incentivize participation. In total, 95% (552 of 579) did the survey with only the updated questions again. We conducted consistency checks against original responses and included an attention check. We discarded the responses from the remaining 5% when analyzing responses to Q2.1 to Q2.8, as their question interpretations might have been inconsistent with ours.

3.3 Survey procedure

The survey was advertised on Prolific as "*Your use of and perspectives on smart devices*" together with a short, high-level description of the task in the respective language. Participants could access the survey after agreeing to the informed consent. The survey was run on Qualtrics (hosted by the research institution) and structured into four sections, which we describe

Demographic		FR	DE	PO	ES	NL	**Total**
Age	18-24	39	41	48	39	43	210
	25-34	41	40	46	40	44	211
	35-44	43	41	43	42	45	214
	45-54	38	40	43	42	41	204
	55-64	25	29	14	33	20	121
	65+	11	9	2	3	8	33
Gender	Female	95	97	93	94	96	475
	Male	98	100	99	100	102	499
	Other response*	4	3	4	5	3	19
		197	200	196	199	201	**993**

Table 2: Demographic overview. *Other responses possible were "*Non-binary/ Third gender*" and "*Prefer not to say*"

in the following.

Participants' own smart device usage. To collect concrete, device-level data on respondents' own smart device usage and duration, the survey began with questions about their own devices. The survey started with a general description of smart devices to provide context, especially for respondents without much experience with such devices. Respondents then indicated the types of smart devices they used and owned and which specific devices they currently used, followed up with more targeted questions about these specific devices, including the model/brand, the condition (new / previously owned), the purchase channel, when it was started being used and for how long looking ahead, and the software updates status (Q2.1 - Q2.8). We asked these follow-up questions only for a maximum of three of their devices (chosen randomly) to keep response time manageable. We also asked if respondents had recently stopped using any smart devices to find out more about their use time, device disposal, and the reasons for ending use (Q4 - Q4.4).

Eliciting lifetime expectations via device vignettes. Respondents were presented with vignettes about different devices to move from their own devices' usage to eliciting their expectations regarding stereotypical device categories. We asked them to imagine they would buy such a device today and emphasized our concept of product lifetime (Q5). Then they were presented with one conventional and two smart device vignettes, both selected randomly from the respective list of devices (see Table 1). The first vignette was a non-smart device to set a baseline and avoid ordering effects by first showing smart devices, as this could easily lead to confusing the subsequent conventional device as being smart.

After each device vignette, participants answered the question: "*If you had to predict, for how many years do you expect such a device to last?*" (Q5.1.1) by entering a whole number in years. We opted for an open-ended response format to avoid potential biases introduced by scale anchors (*anchoring effect* [45]). For instance, an upper anchor such as *"More than 10 years"* might implicitly suggest that 10 years is a long lifespan, thereby lowering lifetime estimates [43]. To capture more contextual data for these numerical lifetime estimations, we also followed up with "*What aspects did you take into account when estimating the number of years?*" (Q5.1.2), where respondents could input their reasoning in an open text field.

Software update and security considerations. In this section, we were interested in respondents' understanding of software support and security aspects for smart devices. As previous work implied that consumers did not fully understand the implications of unsupported smart devices [23], we asked how the end of update support would impact smart devices (Q7) and to what extent respondents had first-hand experience with this (Q7.1), followed by their expectations how long software support would last for the two smart devices they saw earlier in the vignettes (Q8) to see how this estimate would compare to the device's lifetime expectation in Q5.1.1. We then explicitly introduced the concept of security for smart devices with a short explanation (Q9) to then measure respondents' security concerns (Q9.1), mitigation actions (Q9.2), and if a continued provision of security updates would lead them to use their smart devices for longer (Q9.3).

Demographics and survey conclusion After filling out some final demographic questions, respondents were thanked, debriefed, and sent back to Prolific with a completion code to receive payment. The survey included two attention checks (Q3 and Q6). The median completion time was 11.83 minutes. The full survey instrument is provided online[2].

3.4 Data analysis

We first checked the data for suspicious responses by reviewing attention checks, completion time, and spurious patterns like providing the same response continuously or nonsensical open text responses. All respondents who failed both attention checks were removed ($n = 5$). 64 respondents failed one of the two, and after manually reviewing their responses, we removed three due to failing at least one of our removal criteria; repeated scale responses, nonsensical text responses, inconsistencies in responses, such as having started using a device model that was not released yet at this time, or rapid completion times. We also checked the responses of the fastest (< 5 minutes) and slowest (> 1 hour) completion times, but did not find any indications of bogus answers (i.e., they passed both attention checks and gave legitimate text responses). Thus, response quality was generally high, as we only had to remove data from eight respondents.

Quantitative analysis To analyze the data, we first calculated descriptive statistics of survey responses to get an indication of patterns and trends as well as inferential statistics to de-

tect statistically significant differences across responses or countries.

To assess which factors influenced respondents' expectations of devices' lifetimes in the vignettes, we ran a multilevel regression model with maximum-likelihood estimation, allowing us to test for significant differences between devices (both smart and conventional) and account for respondent-level characteristics, respondent-level variance, and model fit. Assumption checks for homoscedasticity, multicollinearity, overfitting, and influential datapoints indicated that lifetime expectations were not normally distributed and displayed a skew towards higher values (e.g., 20 years was not an uncommon response). We thus log- transformed the outcome variable *Lifetime*. For better interpretability, we transformed the resulting coefficient estimates to express percentage changes in the outcome variable (by exponentiation with $e^{\beta} - 1$).

After iteratively adding predictors to the model to assess if goodness of fit improved significantly, we concluded with the final model predicting *Lifetime* with *Device* (the different device vignettes), *Device Experience* (if the respondent used the smart device described in the vignette themselves), *Country*, an interaction between *Country* and *Smartness* (if the device was smart or conventional), and a random effect of respondent to account for individual differences between them. The number of smart device categories used, Age, and Gender showed no effect, as including those predictors did not contribute significantly to the model's fit. The model is presented in Table 4 in the Appendix.

Qualitative analysis Open-text answers were translated into English using the translation tool DeepL [1]. In our Ethical Considerations statement, we detail to how we protected respondents' sensitive data. To ensure quality, the native speakers who were also involved in the survey translation checked a random sample of the resulting translations. The automatic translation performed satisfactorily, with no native speaker reporting any translation errors. Translated text data was then analyzed using thematic analysis [9], where the primary researcher identified and assigned codes to the text answers. After coding a subset of the responses, the resulting initial codebook was discussed at regular intervals with co-authors and refined. After coding approximately one-third of the open text data, we reached theoretical saturation, where no new themes emerged [32], and the codebook was discussed one last time to finalize it. Previous codes were adjusted according to the final codebook, which is provided online[2].

4 Results

4.1 Individual use of smart devices

To address RQ (i) *(How do consumers use their smart devices, and for how long?)* and understand what is a reasonable use time for smart devices and how they are used and purchased, we collected data on survey participants' use of their own smart devices, which resulted in data on 2753 individual IoT devices currently used, and 398 devices used in the past. We also report on relevant country differences throughout this and the following subsections to address Research Question (iv) (*Are there differences among EU member states regarding consumers' smart device usage, expectations, and security and software support perceptions?*).

4.1.1 Devices currently used

On average, respondents indicated using five different smart device categories, with smartphones being the most common, followed by Smart TVs and Routers. Table 3 provides an overview of devices' popularity in the sample. Devices' most popular brands were all from international companies, who will need to comply to the CRA to sell these products in the EU. For some smart devices, especially routers, sensors, doorlocks, doorbells, and solar inverters, a sizable proportion of participants did not know the brand of their currently used device. We added smartphones as an option due to their widespread use and importance in the smart device ecosystem (e.g., due to companion apps).

Device Category	Number	Most common brands	% Unk.
Smartphone	984	Apple, Samsung, Xiaomi	0%
Smart TV	680	Samsung, LG, Sony	3%
Router	611	Fritzbox, TP-Link, Vodafone	37%
Connected printer	582	HP, Canon, Epson	7%
Smartwatch	503	Apple, Samsung, Xiaomi	5%
Media streaming	290	Google, Amazon, Xiaomi	14%
Smart lighting	281	Philips, Ikea, Xiaomi	27%
Smart speaker	281	Amazon, Google, Apple	4%
Robot vacuum cleaner	264	iRobot, Xiaomi, Roborock	11%
Smart security camera	192	Ring, Xiaomi, TP-Link/tapo	27%
Smart sensors	150	Eufy, Kidde, Philips	59%
Smart thermostat	111	Honeywell, Remeha, Tado	34%
Smart washing mach.	108	Samsung, LG, Beko	9%
Smart doorbell	88	Ring, Eufy	33%
Smart hub	48	Google, Philips	21%
WiFi solar inverter	48	Enphase, Solaredge	39%
Smart fridge	42	LG, Samsung, Bosch	5%
Smart doorlock	15	–	43%
Smart baby monitor	14	–	17%

Table 3: Prevalence and brands of smart device categories owned and used by respondents. If fewer than three brands are listed, there are too few observations for a pattern. *% Unk.* is the share of respondents not knowing their device's brand.

To assess how long respondents used their devices, we shifted the level of analysis from device *categories* used to the *particular devices* participants were currently using. We asked if these devices were acquired in new or second-hand condition, as we could not control for the use duration of the previous owner when measuring device use times. This also provided us with valuable insights into the prevalence of the second-hand use of smart devices, as their lifecycle can span different users. The vast majority of smart devices (90%) were reported to have been in new condition, while only 9%

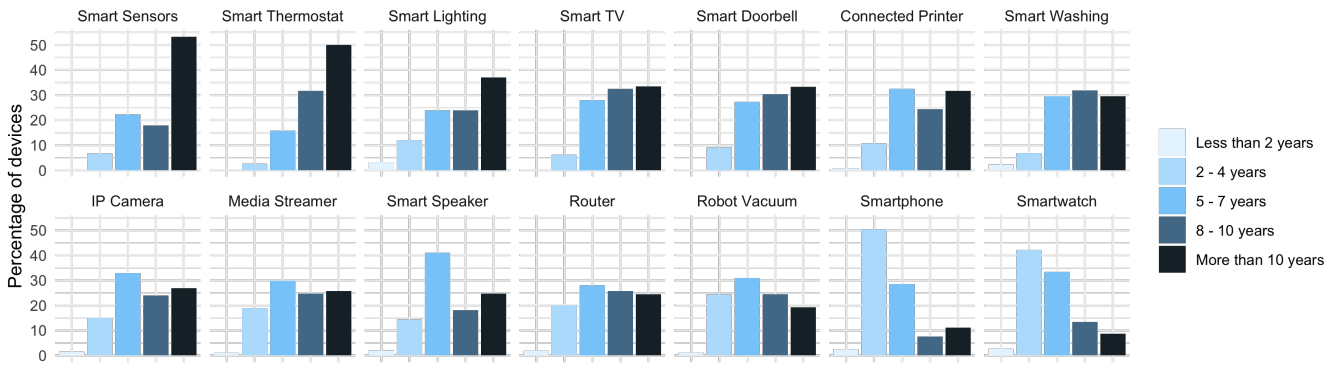

Figure 1: Sum of past use and intended future use duration across respondents' smart devices. Ordered by decreasing rate of durations of more than 10 years. Devices with less than 20 observations are not depicted.

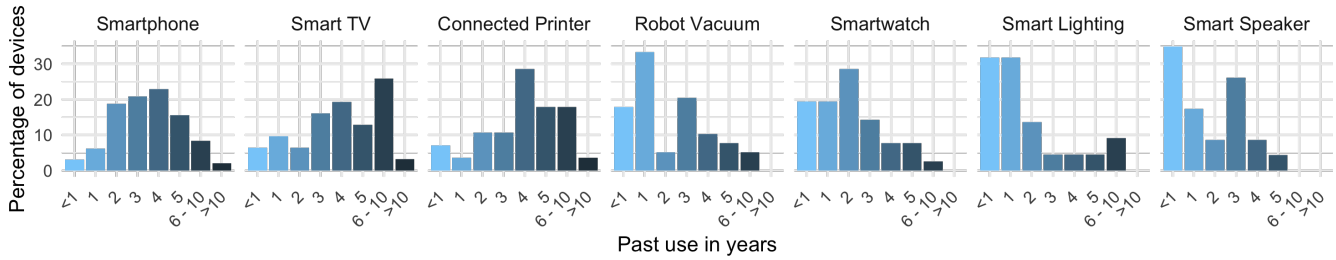

Figure 2: Duration of device usage before stopped being used. Ordered by increasing rate of durations below 1 year.

were previously owned. The devices with the highest rate of second-hand use were smartphones (16%), smartwatches (11%), and smart TVs (9%). For the devices that were new when usage commenced, the majority were purchased in online stores (60%), while physical stores were less popular yet still a sizable amount (30%), highlighting the importance of considering both online and offline sales channels when disclosing support durations to consumers.

There were significant differences between countries regarding smart device purchase channels. Regarding second hand use ($X^2(4) = 28.39$, $p < 0.001$), the highest prevalence was observed in France with 14% of devices being aquired in used condition and the lowest in Spain (5%). Similarly, France had the highest rate of participants selling their previous devices onward (16%). For devices acquired new, the highest proportion of devices bought online was in Poland (69%) and The Netherlands (66%), while the countries with the highest rate of devices bought in physical stores were France (37%) and Spain (35%) ($X^2(8) = 33.47$, $p < 0.001$).

To gauge how long respondents use their current devices, we added the time since they started using them (Q2.2) and for how long they plan to keep using them (Q2.6). We consider this a measure of intended use duration, as it pertains to planned future use, which bears some level of uncertainty. Figure 1 depicts the distributions of past and intended use time across respondents' smart devices. Second-hand devices were not included. Thus, a first differentiation across smart devices in intended use times became evident. Smartwatches and smartphones were clearly skewed towards shorter use times (i.e., mainly in the 2 - 4 years range), while Smart TVs, smart Lighting devices, or smart thermostats showed substantially longer use times on average. Indeed, we found that for the majority of devices except for smartphones and watches, a sizable number of users indicated more than a total of 10 years, indicating long intended use times in terms of smart product standards.

4.1.2 Devices recently stopped to be used

As intended future use can be difficult for individuals to forecast, we also asked respondents about their recently stopped smart devices to assess their recent experience with a device they finished using (Q4.1 - Q4.4), independently whether it was replaced with a newer device or not. In total, respondents reported 398 smart devices they had recently stopped using. The most commonly stopped devices were smartphones ($n = 98$), smartwatches ($n = 81$), and robot vacuum cleaners ($n = 40$). Figure 2 presents the distributions of devices' use times (devices with less than 20 observations are not depicted) and shows that robot vacuum cleaners, smart lighting, smart speakers, and smartwatches were skewed towards shorter use times while smart TVs and printers were often used for longer.

Smartphones were approximately normally distributed around a middle point of four years of use.

The most common reasons why respondents quit using their previous devices were wanting a newer device ($n = 97$, 20% of all reasons provided) and experiencing flaws with the old device ($n = 93$, 19%). Reasons implying a more terminal cause for stopping device use were less common, with 57 (12%) instances of devices stopping working altogether, and 34 (8%) in which incompatibility with other devices or services was the reason. The end of update support ($n = 23$, 5%) and privacy ($n = 26$, 5%) and security concerns ($n = 16$, 3%) were the least common reasons to stop device use.

Similar motivations for device replacement also emerged for respondents who indicated that they already planned to only continue using their current devices for less than a year into the future, in Q2.6. When asked about their motivations, the most prominent reasons were experiencing issues and flaws ($n = 62$, 34%) and desire for a newer device ($n = 48$, 27%). Only 14 participants indicated the end of update support as a reason, and even fewer were due to security and privacy concerns. Thus, users' preference for better alternatives and experiencing functional issues with the current product were the main drivers to stop using their smart devices, rather than update support or security concerns.

Considering what happened to the 398 discontinued devices, the vast majority of respondents indicated they still have them while not actually using them ($n = 190$, 48%). Gifting it to others ($n = 54$, 14%), selling it ($n = 48$, 12%), or discarding it ($n = 33$, 8%) were substantially less likely responses, implying that handing devices on (i.e., gifting or selling it) and subsequent re-use were not common while the vast majority of devices appear to remain with their owner's without being used.

4.2 Lifetime expectations of smart devices

4.2.1 Device level differences

As a respondent's use time of their own device does not necessarily correspond to its expected lifetime (e.g., they could opt to replace and sell it after a short while), we pivot to what respondents expected for how long different device types would generally last for whoever was using them by presenting vignettes of these products. To answer RQ (ii) (*How long do consumers expect different smart device categories to last, and which factors influence these expectations?*) we aimed at learning for how many years participants predicted a range of different smart and conventional device types would last, as elaborated in Section 3.1.1. We supplement these results with qualitative commentary given by respondents when asked what they took into account when estimating devices' lifespans. Table A.4 in the online repository[2] (filename: *Open Text Codes across Devices*) provides the five most commonly mentioned factors per device type taken into account.

Figure 3 presents the expected lifetimes provided for different smart and conventional device categories. The highest expected lifetimes had solar inverters (Conventional: M = 12.65 years, SD = 6.60, Smart: M = 10.75 years, SD = 6.81) and thermostats (Conventional: M = 11.37 years, SD = 5.68, Smart: M = 10.35 years, SD = 6.29). For solar inverters, respondents commonly considered their use case and high expected price as factors (e.g., "*It is an expensive product and should last according to its cost.*" PID678), and for thermostats their usage or perceived lower complexity (e.g., "*That it is a simple device*" PID685), as seen in Table A.4.

Devices with the lowest expected lifetimes were consistently smart. The lowest lifespans were expected for smartwatches (M = 4.84 years, SD = 1.96) and robot vacuum cleaners (M = 5.74 years, SD = 2.51). For both, their continuous use was commonly considered (e.g., a robot vacuum cleaning the floor regularly, a smartwatch worn continuously), while for robot vacuums, environmental factors like animal hair often came up. For smartwatches, however, factors more related to smart device market dynamics were mostly considered: fast innovation cycles, software updates, degrading batteries, and planned obsolescence (e.g., "*Technology changes so fast, it is likely to be obsolete in 5 years*", PID80). Expectations also generally showed less variability for these devices, as evidenced by lower standard deviations and error bars in Figure 3, indicating that expectations reached a stronger consensus among respondents for those products. This was likely due to respondents' more common experience with smartwatches and robot vacuums than for solar inverters and thermostats, as evidenced in their respective prevalence of use (Table 3).

The multi-level regression analysis (Table 4) revealed that differences in expected lifetimes across devices were statistically significant. Taking smart speakers as the reference level (due to their central role in many smart home set-ups and their "important" categorization in the CRA), we found the largest differences to conventional solar inverters (expected to last 56.90% longer) and thermostats (52.70% longer), but also significant differences to other smart devices such as smart washing machines (expected to last 23.20% longer) or smartwatches (expected to last 22.10% shorter). Significant differences thus correspond to the visual trend in Figure 3, where also significant differences are highlighted.

We also found that smart devices had a consistently shorter expected lifetime than their conventional counterparts when considered as a factor. Most smart devices (except for smoke detectors and printers, with a marginal difference) had a lower average reported lifetime, an effect that was statistically significant (-17.1%, t(2972) = - 9.82, $p < 0.001$). We identified several drivers for this, such as the added complexity of smart features ("*Adding [smart] functions risks making them even more susceptible to problems.*" PID564), software updates, or potential incompatibility, but also some more complex dependencies were taken into account, like "*The company selling this machine will go bankrupt, and we won't be able to install*

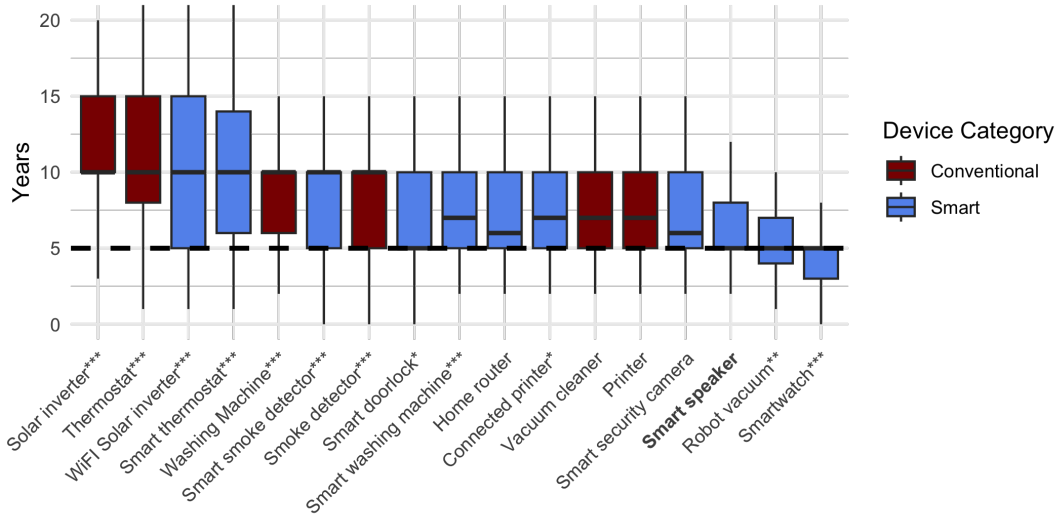

Figure 3: Expected lifetimes for different smart and conventional device categories ordered by mean expected lifetime. Responses were given as whole numbers. The dashed horizontal line denotes the CRA's five-year baseline, and asterisks significant differences to the reference level *Smart speaker*.

the application on updated OS versions." (PID21).

As can also be derived from Table A.4 , devices' *Usage* and *Device type* were generally among the most common factors considered by participants when estimating lifespans across all devices. While static device qualities such as the type of device ("Washing machines last a long time") can be seen as more straightforward heuristic for the lifespan, usage ("How often the washing machine runs") is less deterministic, as this depends on wear and tear of components, how frequently and intensively the user decides to use the device, and if it is used as intended or not.

4.2.2 Individual differences

Lifetime expectations were also strongly affected by respondent-level factors besides device-related aspects. The regression model fit coefficients provided in Table 4 suggest that when accounting for respondent-level variation, the model fit (Conditional R^2: 46.40%) increased substantially in contrast to only considering the device, country, or own experience with the device (Marginal R^2: 16.60%). This highlights the substantial impact of individual differences and the subjective nature of lifespan expectations for products. Some respondents consistently expected longer lifespans across devices, while others had a tendency to expect shorter lifespans, indicating systematic variation in personal perceptions.

Also personal experience with the smart device affected expectations - Respondents who used the same device type themselves as described in the vignette at hand expected longer lifespans on average than participants who did not (8.0% longer, $p < 0.01$), possibly due to familiarity with the device or increased optimism due to personal investment in it. However, we found no effect of experience with smart devices in general (i.e., the number of smart device types the participant was using), implying that the user's experience with the same device category was a stronger predictor for expected lifetimes.

We also found significant differences between countries in how long respondents expected devices to last. Taking Spain as the reference, respondents in Poland generally expected devices to last significantly shorter (14.1% less, $p < 0.001$), while participants in The Netherlands and Germany had more optimistic expectations (9.2% and 8.6% longer, respectively). However, an interaction between country and the smartness of the product indicated that in these two countries, respondents expected smart devices to last significantly shorter than conventional devices compared to Poland (Germany: 8.5% shorter, The Netherlands: 12.2% shorter). Thus, participants in Germany and The Netherlands were comparatively more skeptical about the lifespan of smart devices. Age and Gender had no effect on expected lifetime.

4.3 Perceptions of software updates and security over devices' lifetime

As the previous analyses focus on smart devices' use times and expected lifetimes to measure what constitutes a reasonable lifetime, we now focus specifically on the role of software updates and security aspects over devices' lifespan to answer RQ: (*iii*) *How do consumers perceive security and software update support over smart devices' lifespans?*

4.3.1 Update expectations and experiences

In contrast to the static nature of most conventional, non-smart devices, smart devices can be under continuous modification due to software updates. We were thus interested in understanding how consumers perceived update-induced changes to devices over their lifespan and how their subsequent end would affect the user's experience with the product.

More than half of respondents ($n = 533$, 54%,) expected the software update support to correspond with the device's full lifespan, as they provided the same value for both (Q5.1.1 and Q8). When directly asked for their expectations on how the end of update support would impact smart devices' use, no new features ($n = 853$, 86% of participants) and incompatibility with other devices and services ($n = 752$, 76%) were the most commonly expected changes, while almost no participant expected no changes (Figure 4). Interestingly, both security-related answer options (no more fixes to vulnerabilities and no more risk monitoring for the device) were also commonly expected ($n = 714$ and $n = 705$, respectively), despite the survey not mentioning security or privacy up to this point and answer order randomization. Thus, approximately 70% of the respondents were indeed aware of the security implications that the end of update support brings with it.

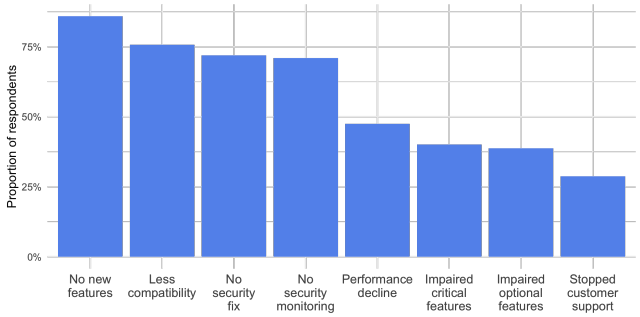

Figure 4: Changes to smart devices after software support ends as expected by respondents (in %). The order of the options was randomized. Multiple choices were possible. The responses "*I don't expect any changes*", "*Not sure*", and "*Other*" were below 1% and omitted from this plot.

To check respondents' own experiences with end-of-support-induced changes, we also asked if they had experienced their previously provided expected changes with their own devices. Figure 5 shows that no new features, a declining device performance, and less compatibility with other devices and services had the highest proportion of respondents experiencing this. We also saw the potential role of ended support for product obsolescence: Among the participants who expected critical features to stop working at this point, around half actually experienced this, so their devices' functionality was essentially made obsolete after not receiving updates.

While such functional impacts on the device were thus quite apparent, security-related changes were more subtle and

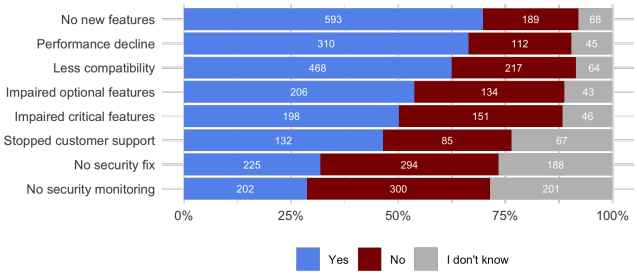

Figure 5: Respondents' own experiences with changes to their devices after the end of update support. They were asked: "*Did you experience any of these changes with your devices yourself?*"

imperceptible for users. Both security-related answer options (no more fixes to vulnerabilities and No more risk monitoring for the device) had the highest rates of respondents indicating not experiencing them or not being sure, while they both were frequently expected as a common change after the end of support (see Figure 4), highlighting how opaque security (and its absence) can be for smart device users.

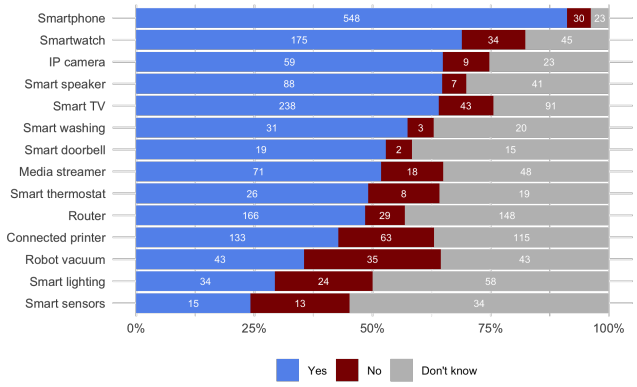

Figure 6: Responses to the question: "*Does the particular device you are currently using still receive software updates, as far as you know?*" Devices with less than 20 observations were not included.

Related to this imperceptibility of updates, Figure 6 shows substantial differences in the current update support status across the smart devices used by respondents. For smartphones, the vast majority indicated the device to still be receiving updates, while for many other smart devices a substantial proportion of participants reported not knowing if it still was. For instance, for smart sensors and lighting products, at least half of respondents indicated they did not know if the device still received updates. Indeed, this uncertainty of the device's update status was much more prevalent than unsupported devices still being used (with robot vacuum cleaners having the highest proportion of unsupported devices). Thus, while the

majority of respondents' smart devices were reported to still be supported, it also illustrates the challenge for users to actually *know* whether their smart devices still receive updates, especially for devices with limited user interfaces like sensors, lighting, doorbells, or routers.

4.3.2 Security and Privacy perceptions and behaviors

As a majority of respondents were aware of the security implications of the end of support, although often imperceptible, we now focus on their security and privacy-related perceptions towards smart devices.

Figure 7 suggests that when prompted for security-related concerns about their own smart devices, respondents mostly indicated to be concerned about their personal data ("*My personal data being accessed by unauthorized individuals*" = 57% of respondents, "*More personal data collected from the device than I expect*" = 56%, "*My personal data being shared with third parties by the manufacturer without my consent.*" = 52%). Two of these were actually privacy-related concerns, with the device's vendor as the "perpetrator". The device being directly attacked and leveraged maliciously was also a common concern (50%), while the device being damaged by an attack (30%) or insufficient customer support in case of an attack (23%)were expected less often. Not being concerned was the least selected response (15%).

To address such concerns, respondents indicated to apply varying mitigation actions, as depicted in Figure 8. The importance of updates became evident, as installing the latest software update was the most prominent mitigation behavior and reported by 56% of respondents ($n = 552$). Stopping to use the device altogether after software support ends was the least common behavior ($n = 121$), yet still selected by approximately 12% respondents. This was in line with our previous finding that the end of software support or concerns about privacy or security were not prominent reasons to stop using a device.

When asked if respondents would use their smart devices for longer if they continued to receive *security* updates (Q9.3), the vast majority strongly agreed or agreed (78%). This seemed to be a contradiction at first, as the end of update support was not a common reason for respondents to stop using their devices nor a trigger to stop using the device to address security concerns.We interpret this finding such that as longer patching support will give reassurance to users that they can safely *continue* using their devices if they want to, its end was not a strong enough trigger for users to *quit* using them. We also note the importance of the device's brand and its associated trustworthiness for respondents to avoid security risks (53%, n = 528).

We also found significant country differences in how participants reported to address their concerns (X^2 (24) = 38.03, $p < 0.05$). Installing the latest updates was reported the most common mitigation in the Netherlands (24%) and Germany (23%), but less so in Poland (19%), where, as well as in Spain, being cautious about how using the device and choosing trustworthy brands were more popular.

5 Discussion

In this survey study ($n = 993$), we empirically explored consumers' usage and expectations of smart devices and their lifespans in the EU, to address the uncertainty around the abstract legal concept of reasonable user expectations. The Cyber Resilience Act [49] aims at converging security support duration with smart device lifetimes, and requires manufacturers to consider reasonable user expectations when defining this period – a policy with global ramifications for the smart device market. For instance, practically all brands of respondents' smart devices were from large, globally active manufacturers, who will have to comply and could thus also uphold support in other markets.

5.1 Device lifetimes

We found that all smart devices included in this survey (except smartwatches) were on average expected to last longer than the CRA's minimum support period of five years, despite many participants considering factors artificially reducing product lifetime, such as a premature replacement for newer alternatives or planned obsolescence. Smart products were also commonly used by respondents for a period longer than this, with use times well above 10 years common for some devices. Surprisingly, a majority (54%) of participants actually expected the update support period to correspond to the smart device's full lifetime, which contrasts with current practices in the smart device market [18, 39, 42], but highlights the importance of aligning support periods to be closer to device lifetime to meet expectations.

Previous work found that device re-use is a common practice, with the first owners often gifting or selling their devices onwards [25, 29]. We found this was present but not substantial in our sample. 9% of respondents' own devices were second-hand, and selling or gifting a previously used device was by far not as common as retiring it at home without using it. Still, second-hand use or repair [10, 50] are conceivable practices, perhaps due to economic reasons (e.g., for low-income users [27]) or sustainability considerations, increasing device use times. It is unclear to what degree second-hand use and repairability will be factored in when manufacturers, market surveillance authorities, or courts determine expected use time and support period.

5.2 Software Updates and Security over devices' lifespan

"Smart" factors such as software updates, incompatibility, or added complexity led to smart devices being expected to have

shorter lifetimes than conventional products (Section 4.2.1). However, the central role of software updates for security was often seen. In contrast to a commonly reported unawareness or uncertainty of updates among users in previous research [11, 16, 23, 24], we found that respondents generally exhibited awareness of updates' security implications. 70% expected no more security reassurances after update support ended, and installing the latest updates was reported as the most common mitigation to address security concerns. As there are some differences in our study's demographics in contrast to this previous work, with participants in [23, 24] being US-based smart home users with limited security experience, [16] studying young users of widely used software, and [11] practitioners at UK router vendors indirectly describing their users, it raises the question if this effect was due to differences in samples and or if this awareness might actually be increasing over time.

However, while an association between end of update support and security implications was arguably observable in our study, security concerns were weak triggers for respondents to stop using a device. More attractive alternatives or declining functional performance were the prevalent drivers. This was likely amplified by the imperceptibility of updates and security measures. For many of their own devices, respondents did not know if the device was still supported, or did not experience or know about security support stopping.

Thus, a key challenge with prolonged support duration is ensuring visibility to users. Currently, indicators of software versioning and update status are often unclear or inconsistent across smart devices (as observed in our work and in, e.g., [22–24]), which often lack a user interface. It is challenging for users to verify if a manufacturer is maintaining security updates as promised, potentially leading to a form of learned helplessness akin to delegation of security responsibilities [13], where users must rely on manufacturers' assurances without a straightforward means of verification for themselves. While the CRA sets requirements on update delivery and notifications (to be automatic by default, with notification channels to users available, e.g., to opt-out), it remains an open question through which mechanisms - if any - users can actively engage and hold manufacturers accountable for ongoing security support, comparable to other regulatory frameworks such as GDPR [47], where subject access requests can be submitted to obtain data about themselves.

As the CRA is still in a nascent stage, guidance about support periods will be crucial in the coming years before the market converges on expected support times for "products with digital elements" in all their forms. Guidance will reduce uncertainty and avoid courts having to eventually make the case for what constitutes a reasonable use time and which elements of a product determine this. Our work contributes to this ongoing conversation by empirically assessing device use times and expected lifetimes for a range of different smart product categories and what factors consumers take into account, as information valuable for manufacturers, market authorities, and the EU administrative cooperation group (ADCO), who will publish guidance on support times in the coming years.

5.3 Recommendations

Here we discuss initial recommendations emerging from our work.

Manufacturers: For manufacturers, users' expectations take center stage in product conformity with the CRA; manufacturers will now need to document how they consider these expectations when determining support periods.

Going beyond device-internal usage data. Our work demonstrates that for a meaningful understanding of users' expectations, getting in contact with them is essential, as relying exclusively on internal device usage data (i.e., device logs how long it is used) might be insufficient to account for expectations, as other contributing factors emerged from our data. For instance, respondents differentiated between smart and non-smart products and considered factors such as the device's price, perceived quality, or environmental factors of usage. Also, the duration how long device data can be collected is arguably determined by the manufacturer, not by expectations. We thus recommend that manufacturers leverage sales channels as well as market and user research capabilities to learn about and document their customers' lifetime expectations for the respective product categories. As our data exhibited substantial individual and country differences, we advise applying a sampling strategy that considers countries, user demographics, and sufficient sample sizes.

Reducing user uncertainty. Furthermore, our results suggest that ongoing security support for smart devices is often indistinct to users, as evidenced by high proportions of users not being sure about the update status of their own devices (Figure 6) and experiencing uncertainty with respect to the end of update support (Figure 5). Thus, tangible factors demonstrating competence to provide support should be made salient by manufacturers at the time of device adoption and over the device's lifetime, possibly woven into marketing, product disclosure, and easy-to-access support status indications of the product (e.g., via a companion app). As we also found that choosing trusted brands was a major way for respondents to navigate security concerns (Figure 8) and a clear preference for longer support periods (as also suggested by previous work [15, 33, 35]), a stance of active security support has marketing and brand-building potential.

Policymakers and market surveillance: Approaching consumer expectations. Market surveillance authorities in EU member states should note that expected lifetimes and actual use times of consumer smart devices were commonly found to be higher than the CRA's baseline of five years (Figure 1, 2 and 3). The EU administrative authorities (ADCO)

can publish guidance on reasonable support durations for different product categories, or, if "data suggests inadequate support periods for specific categories of products" (Article 52(16) & Recital 62) issue recommendations to market surveillance authorities to focus on those products or to the EU Commission to delegate acts and define minimum support durations. Our data should thus be considered as a first indication that several smart product categories considered in this study require delineation from the baseline of five years as suggested in the CRA. Additionally, they should be aware of a potentially self-defeating dynamic for consumers regarding expected smart device lifetimes: Smart versions of a product category were expected to last shorter on average than conventional counterparts, and participants considered factors they are accustomed to from the current smart device market; quick replacement, emerging incompatibility with other products, or planned obsolescence. As these are factors artificially reducing use times and thus not justifying a product's definite end of life (and smart devices being repaired, resold, and reused, as we also found in our study), policymakers and market authorities should be cautious to consider such dynamics when user expectations are measured or defined.

Providing assurances to users. The CRA's support duration provisions will likely lead to longer support with security updates to smart devices, exposing them to continuous modification. We found that participants experienced phenomena with their devices over their use time that may or may not relate to (the end of) security updates, like declining performance, less compatibility, impaired features, or simply being unsure (Figure 5). Thus, policymakers and market authorities should consider defining assurances for users over the devices' lifetime that manufacturers should provide. This could include explicitly calling out potential "side effects" how the update could affect the device's behavior via notifications accompanying updates. As the CRA also requires security updates to be published separately from functionality updates where technically feasible (Annex I, Part II (2)), we recommend market authorities to explicitly consider this legal instrument to reduce such in-transparency for users.

5.4 Limitations

A survey relies on self-reporting, and for some responses, such as whether longer security support leads to prolonged device use, it remains uncertain if this translates to actual behavior. Additionally, the survey topic and some questions were complex. For example, recalling the year a device was first used or whether it still receives updates could be difficult for respondents. We did not filter for smart device ownership, and while most respondents used at least one device, concepts like smartness, updates, and security could be challenging. To mitigate this, we used simple language, refined the survey through iterations, conducted a pilot study, and provided definitions and "I don't know" options.

Sampling and generalizability are further limitations. Our sample is not representative of the general EU population or the included countries, and we only studied a subset of product categories falling under the CRA. As a common limitation in such online surveys, participants on Prolific tend to be younger and more technologically knowledgeable than the general population [44], leading to an underrepresentation in our study of those over the age of 55, despite aiming for a balance across age groups and genders. However, even with a sample of participants with an arguably higher technological literacy, we observed high levels of uncertainty towards participants' awareness of their devices' support (e.g., Figure 6). Resource constraints also limited our survey delivery to a subset of five member states (with Section 3 explaining our rationale). We thus invite future work to extend our methodology to other countries and products with digital elements, as the CRA will apply to a plethora of products, not just consumer smart devices.

Lastly, many factors can influence a device's expected lifespan, including usage, environment, quality, and price. Our vignettes focused only on device type, exploring additional factors through qualitative responses. Future work could adopt more complex vignette designs incorporating variables such as brand, price, and usage.

6 Conclusion

The upcoming Cyber Resilience Act will increase the responsibilities of manufacturers of smart consumer devices and market surveillance authorities in the EU to determine and uphold the update support periods of smart products. In contrast to other legislation, where disclosure on support periods via product labels is prominent [17,46], the CRA will require manufacturers to actually uphold a certain support period. In contrast to the previous status quo, this will involve considering users, as reasonable user expectations regarding the product's lifetime will have to be considered when determining the support period.

In this work, we empirically assess user expectations and behaviors regarding smart devices' lifetimes, support durations, and security considerations to provide insights into this abstract legal notion. We find that expectations vary for different (smart) device categories, with smart devices generally being expected to last shorter than their conventional counterparts. We also find that a prolonged support duration harmonizes with users' expectations.

Acknowledgments

This work has been partially supported by the INTERSECT project, Grant No. NWA.1160.18.301, funded by Netherlands Organisation for Scientific Research (NWO). The findings reported herein are solely responsibility of the authors.

Ethical Considerations

This research adheres to the principles of "*Beneficence*", "*Respect for Persons*", "*Justice*", and "*Respect for Law and Public Interest*" as in the Menlo report [26].

Beneficence: To appropriately balance probable harm and the likelihood of enhanced welfare resulting from our research, we carefully considered the related EU legal system and how our research could have an effect on the rights of consumers of smart devices. We see the possibility for societal benefits in our work, as our empirical analysis provides users a voice in ongoing and future discussions on support durations, and could also be considered by market authorities and manufacturers to define *longer* security support, as we also directly consider second-hand use and repairability. For this reason, we state that our results pose a conservative estimate, which could be increased.

Respect for persons: As our research involved human subjects, we deployed several safeguards to respect their rights. Before conducting the survey, we obtained approval from our Institutional Review Board (IRB), which also required a data management plan to detail how data was collected, stored, and used. The application to the IRB also included a comprehensive checklist for human subject research, where possible harms and risks had to be explicitly identified and mitigated. These documents for the IRB application were reviewed and approved by a data protection steward and the IRB.

To ensure informed consent, participants had to read and accept the IRB-approved consent form before starting the survey. This outlined survey purpose, estimated duration, data usage and storage, voluntary participation with the option to withdraw (resulting in data exclusion), and the collection of non-identifiable demographic information (e.g., age ranges, as optional responses). Data was stored on an encrypted institutional network, accessible only to the research team. Researcher contact details were provided for any inquiries.

We only used mild deception, as we did not immediately disclose to participants that the survey was also about security aspects of smart devices. This was so as not to bias their responses, and we gave a full disclosure at the end of the survey, to serve as a debrief. This is the typical extent of deception for human-subjects studies.

To protect respondents' right to privacy, we did not collect any PII in the survey explicitly. However, despite our best efforts, open-text responses can constitute indirect identifiers in combination with other data, for instance specific device models or store names. We then erred toward privacy preservation and do not share raw data. To translate open-text survey responses (to Q5.1.2 and Q8.1) with DeepL, we used an advanced membership, which included using TLS encrypted connection during storage and transfer to servers based in the EU and immediate deletion of any text after translation. DeepL is a Germany-based company adhering to GDPR and is ISO 27001 certified. Furthermore, as open-text responses were translated in isolation (i.e., not in combination with any other survey responses), an identification of any participant's identity would not be possible.

To pay respondents fairly for their time and effort, we paid them an hourly rate according to the minimum wage in the research institution's country. In the pilot study, we paid for 25 minutes; in the final survey, for 18 minutes; and in the short follow-up survey with updated Q2 – Q2.8, for 4 minutes. We took generous estimates on completion time. The median of the final survey was 11 minutes (3rd quartile: 16 minutes) instead of 18. Thus, we effectively paid the vast majority of participants more than minimum wage.

Justice: We aimed at fairly distributing risks and benefits across stakeholders by including recommendations for both manufacturers and policymakers, as well as including consumers as participants to give them an active voice in the ongoing and future conversations around support periods.

Respect for Law and Public Interest: In public interest, we did not want our results to give an argument to reduce device lifetimes artificially to comply with the CRA. For instance, as we found smartwatches were expected to have short lifetimes (shaped by current and unsustainable market practices), we did not want to provide an argument for vendors to reduce smartwatches' lifetime or keep them low. To address this, we reiterate that we only provide a starting point for manufacturers and market surveillance authorities on how to conceptualize user expectations via empirical insights for consideration when determining the support period. Only the courts can interpret the CRA and determine what constitutes a reasonable support period for a given product. We also explicitly stress that factors such as fast replacement or planned obsolescence are not valid factors to consider when determining the support period, and that most participants considered the device type and its usage instead, as also defined in the CRA as critical criteria. Further, we emphasize the preference of users for longer support times and the heightened transparency via the CRA and other labeling policies, thus highlighting the "costs" for manufacturers' reputations when keeping support times short.

Open Science

For other researchers to replicate or build on our work, we explain our methodology in Section 3, and provide the survey instrument, vignettes, and the resulting codes from open-text responses in an online repository[2]. There, we also share survey results in aggregated form across categories and dimensions such as device types or multiple choice responses, thereby also including the source data for most of the plots. As explained in respecting respondents' privacy, based on our data protection steward's advice, we opted to take a more conservative stance to preserve privacy due to open text responses and potential indirect identifiers in them when applying for IRB approval.

References

[1] DeepL translator. URL: https://www.deepl.com/en/translator.

[2] Noura Abdi, Xiao Zhan, Kopo M Ramokapane, and Jose Such. Privacy norms for smart home personal assistants. In *Proceedings of the 2021 CHI conference on human factors in computing systems*, pages 1–14, 2021.

[3] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(2):1–23, 2018. doi:10.1145/3214262.

[4] Katrin Auspurg and Thomas Hinz. *Factorial survey experiments*, volume 175. Sage Publications, 2014.

[5] Paritosh Bahirat, Martijn Willemsen, Yangyang He, Qizhang Sun, and Bart Knijnenburg. Overlooking Context: How do Defaults and Framing Reduce Deliberation in Smart Home Privacy Decision-Making? In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–18. ACM, 2021. doi:10.1145/3411764.3445672.

[6] Jeff Bennett and Vic Adamowicz. Some fundamentals of environmental choice modelling. *The choice modelling approach to environmental valuation*, pages 37–69, 2001.

[7] Anu Bradford. *The Brussels Effect: How the European Union Rules the World*. Oxford University Press, 2020.

[8] Conner Bradley and David Barrera. Escaping Vendor Mortality: A New Paradigm for Extending IoT Device Longevity. In *Proceedings of the 2023 New Security Paradigms Workshop*, NSPW '23, pages 1–16, New York, NY, USA, December 2023. Association for Computing Machinery. URL: https://dl.acm.org/doi/10.1145/3633500.3633501, doi:10.1145/3633500.3633501.

[9] Virginia Braun and Victoria Clarke. One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative research in psychology*, 18(3):328–352, 2021.

[10] Jason Ceci, Jonah Stegman, and Hassan Khan. No privacy in the electronics repair industry. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 3347–3364. IEEE, 2023.

[11] G. Chalhoub and A. Martin. But is it exploitable? Exploring how Router Vendors Manage and Patch Security Vulnerabilities in Consumer-Grade Routers. *European Symposium on Usable Security (EuroUSEC 2023)*, pages 277–295, 2023.

[12] Jayne Cox, Sarah Griffith, Sara Giorgi, and Geoff King. Consumer understanding of product lifetimes. *Resources, Conservation and Recycling*, 79:21–29, 2013.

[13] Paul Dourish, Rebecca E Grinter, Jessica Delgado De La Flor, and Melissa Joseph. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8:391–401, 2004.

[14] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. Ask the Experts: What Should Be on an IoT Privacy and Security Label? In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 447–464, 2020. doi:10.1109/SP40000.2020.00043.

[15] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–12. ACM, 2019. doi:10.1145/3290605.3300764.

[16] Michael Fagan, Mohammad Maifi Hasan Khan, and Ross Buck. A study of users' experiences and beliefs about software update messages. *Computers in Human Behavior*, 51:504–519, October 2015. URL: https://www.sciencedirect.com/science/article/pii/S0747563215003854, doi:10.1016/j.chb.2015.04.075.

[17] Federal Communications Commission (FCC). U.S. Cyber Trust Mark, 2024. URL: https://www.fcc.gov/CyberTrustMark#:~:text=The%20program%20applies%20to%20consumer,door%20openers%2C%20and%20baby%20monitors.

[18] Federal Trade Commission. Smart Device Makers' Failure to Provide Updates May Leave You Smarting, 2024. URL: https://www.ftc.gov/reports/smart-device-makers-failure-provide-updates-may-leave-you-smarting.

[19] Alex Gnanapragasam, Christine Cole, Jagdeep Singh, and Tim Cooper. Consumer perspectives on longevity and reliability: a national study of purchasing factors across eighteen product categories. *Procedia Cirp*, 69:910–915, 2018.

[20] Alex Gnanapragasam, Masahiro Oguchi, Christine Cole, and Tim Cooper. Consumer expectations of product lifetimes around the world: a review of global research findings and methods. *PLATE: Product Lifetimes And The Environment*, pages 464–469, 2017.

[21] Julie Haney, Yasemin Acar, and Susanne Furman. "It's the Company, the Government, You and I": User Perceptions of Responsibility for Smart Home Privacy and Security. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 411–428, 2021.

[22] Julie M Haney and Susanne M Furman. Work in Progress: Towards Usable Updates for Smart Home Devices. In *International Workshop on Socio-Technical Aspects in Security and Trust*, pages 107–117. Springer, 2020. doi:10.1007/978-3-030-79318-0_6.

[23] Julie M. Haney and Susanne M. Furman. Smart Home Device Loss of Support: Consumer Perspectives and Preferences. In *HCI for Cybersecurity, Privacy and Trust: 5th International Conference, HCI-CPT 2023, Held as Part of the 25th HCI International Conference, HCII 2023, Copenhagen, Denmark, July 23–28, 2023, Proceedings*, pages 492–510, Berlin, Heidelberg, July 2023. Springer-Verlag. doi:10.1007/978-3-031-35822-7_32.

[24] Julie M. Haney and Susanne M. Furman. User perceptions and experiences with smart home updates. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 2867–2884, 2023. doi:10.1109/SP46215.2023.10179459.

[25] harris interactive. Consumer Internet of Things Security Labelling Survey Research Findings, 2019. URL: https://assets.publishing.service.gov.uk/media/5ff713bfe90e0763a31280a1/Harris_Interactive_Consumer_IoT_Security_Labelling_Survey_Report_V2.pdf.

[26] Erin Kenneally and David Dittrich. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research, August 2012. URL: https://papers.ssrn.com/abstract=2445102, doi:10.2139/ssrn.2445102.

[27] Anastassija Kostan, Sara Olschar, Lucy Simko, and Yasemin Acar. Exploring digital security and privacy in relative poverty in germany through qualitative interviews. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 2029–2046, 2024.

[28] Lorenz Kustosch, Carlos Gañán, Mattis van 't Schip, Michel van Eeten, and Simon Parkin. Measuring up to (reasonable) consumer expectations: Providing an empirical basis for holding IoT manufacturers legally responsible. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 1487–1504, Anaheim, CA, August 2023. USENIX Association. URL: https://www.usenix.org/conference/usenixsecurity23/presentation/kustosch.

[29] Peiyu Liu, Shouling Ji, Lirong Fu, Kangjie Lu, Xuhong Zhang, Jingchang Qin, Wenhai Wang, and Wenzhi Chen. How IoT Re-using Threatens Your Sensitive Data: Exploring the User-Data Disposal in Used IoT Devices. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 3365–3381, May 2023. ISSN: 2375-1207. URL: https://ieeexplore.ieee.org/abstract/document/10179294?casa_token=T6tqj4aLNdgAAAAA:gNWxmBMwzQVvsrwrp7eGnVvFRvWNjCCFe68kBXHxtRq-2j2bYnyKwDYKlJPovvmIKu_lsZ4, doi:10.1109/SP46215.2023.10179294.

[30] René Mahieu, Hadi Asghari, Christopher Parsons, Joris van Hoboken, Masashi Crete-Nishihata, Andrew Hilts, and Siena Anstis. Measuring the Brussels Effect through Access Requests: Has the European General Data Protection Regulation Influenced the Data Protection Rights of Canadian Citizens? *Journal of Information Policy*, 11:301–349, December 2021. doi:10.5325/jinfopoli.11.2021.0301.

[31] Megan Crouse. WUS to Launch Cyber Trust Mark to Label Secure Smart Devices, 2025. URL: https://www.techrepublic.com/article/us-cyber-trust-mark-iot-security/.

[32] Sharan B. Merriam and Elizabeth J. Tisdell. *Qualitative Research: A Guide to Design and Implementation*. John Wiley & Sons, August 2015. Google-Books-ID: JFN_BwAAQBAJ.

[33] Philipp Morgner, Christoph Mai, Nicole Koschate-Fischer, Felix Freiling, and Zinaida Benenson. Security Update Labels: Establishing Economic Incentives for Security Patching of IoT Consumer Products. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 429–446, 2020. doi:10.1109/SP40000.2020.00021.

[34] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. Privacy expectations and preferences in an IoT world. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 399–412, 2017.

[35] Majid Nasirinejad and Srinivas Sampalli. Evaluating Consumer Behavior, Decision Making, Risks, and Challenges for Buying an IoT Product. *IoT*, 4(2):78–94, 2023.

[36] Daisuke Nishijima and Masahiro Oguchi. Measuring product lifetime extension potential by increasing the expected product lifetime: Methodology and case study. *Business Strategy and the Environment*, 32(4):1218–1231, 2023.

[37] Dawn Carla Nunziato. The Digital Services Act and the Brussels Effect on Platform Content Moderation. *Chi. J. Int'l L.*, 24:115, 2023. URL: https://cjil.uchicago.edu/print-archive/digital-services-act-and-brussels-effect-platform-content-moderation.

[38] Masahiro Oguchi, Tomohiro Tasaki, Ichiro Daigo, Tim Cooper, Christine Cole, and Alex Gnanapragasam. Consumers' expectations for product lifetimes of consumer durables. In *2016 Electronics Goes Green 2016+(EGG)*, pages 1–6. IEEE, 2016.

[39] Privacy International. We looked into the software support practices for 5 of the most popular smart devices (and the results may disappoint you), 2022. URL: https://privacyinternational.org/report/4965/we-looked-software-support-practices-5-most-popular-smart-devices-and-results-may.

[40] Prolific. URL: https://www.prolific.co/.

[41] Qualtrics. Qualtrics translate survey. URL: https://www.qualtrics.com/support/survey-platform/survey-module/survey-tools/translate-survey/.

[42] Dan Robinson. Nice smart device – how long does it get software updates?, 2023. URL: https://www.theregister.com/2023/01/16/smart_device_software_support/.

[43] Norbert Schwarz, Hans-J Hippler, Brigitte Deutsch, and Fritz Strack. Response scales: Effects of category range on reported behavior and comparative judgments. *Public opinion quarterly*, 49(3):388–395, 1985.

[44] Jenny Tang, Eleanor Birrell, and Ada Lerner. Replication: How Well Do My Results Generalize Now? The External Validity of Online Privacy and Security Surveys. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 367–385, 2022.

[45] Roger Tourangeau, Lance J. Rips, and Kenneth Rasinski. *The Psychology of Survey Response*. Cambridge University Press, March 2000. Google-Books-ID: bjVYdyXXT3oC.

[46] UK National Cyber Security Center. Smart devices: new law helps citizens to choose secure products, 2024. URL: https://www.ncsc.gov.uk/blog-post/smart-devices-law.

[47] European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). *Official Journal of the European Union*, 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[48] European Union. Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC (Text with EEA relevance.). *Official Journal of the European Union*, 2019. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019L0771.

[49] European Union. 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) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). *Official Journal of the European Union*, 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454.

[50] Tanvi Vats, Neelima Sailaja, and Fabiana Anselmo Polido Lopes. Exploration of User Perspectives around Software and Data-Related Challenges Associated with IoT Repair and Maintenance against Obsolescence: User Study on Software and Data Interactions and Considerations for IoT Repair and Maintenance against Obsolescence. In *Proceedings of the 13th Nordic Conference on Human-Computer Interaction*, pages 1–17, 2024.

[51] Harald Wieser, Nina Tröger, and Renate Hübner. The consumers' desired and expected product lifetimes. *Product Lifetimes And The Environment*, 2015.

A Appendix

A.1 Additional Figures

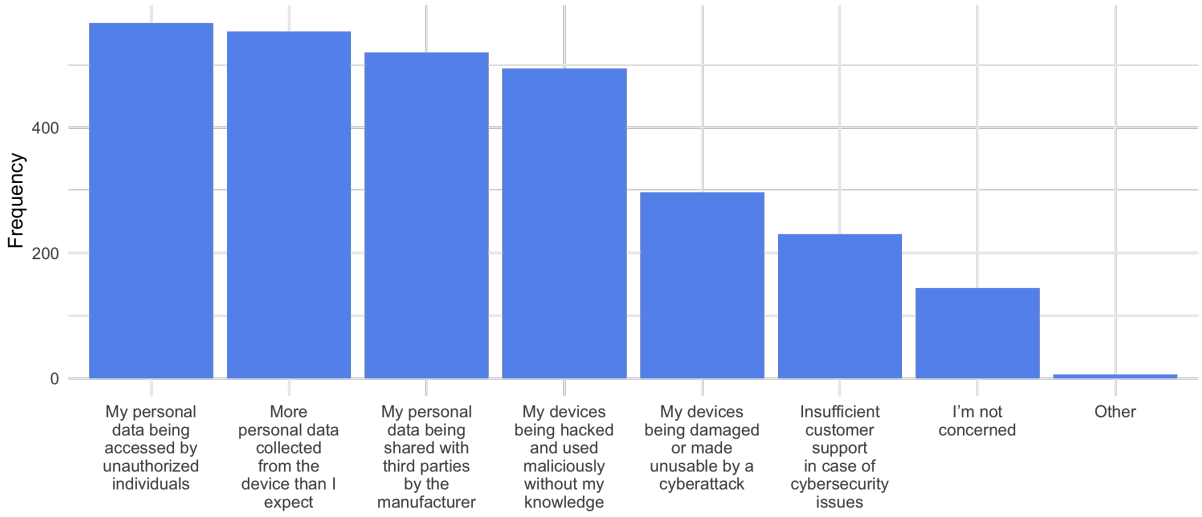

Figure 7: Respondents' concerns relating to security and privacy risks with their smart devices. The order of the options was randomized. Multiple choices were possible.

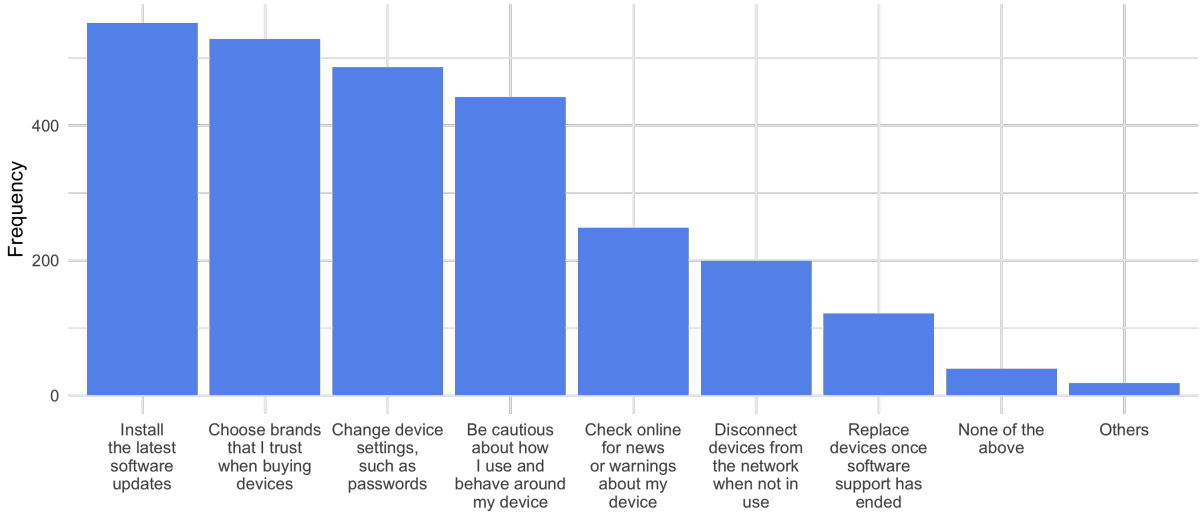

Figure 8: Respondents' mitigation behaviors relating to their security and privacy concerns with their smart devices. The order of the options was randomized. Multiple choices were possible.

A.2 Regression Table

	Coefficient	Standard error
Intercept	6.431^{***}	0.054
Device Type *(Ref: Smart speaker)*		
Conventional printer	0.072	0.052
Conventional smoke detector	0.211^{***}	0.053
Conventional solar inverter	0.569^{***}	0.053
Conventional thermostat	0.527^{***}	0.053
Conventional vacuum cleaner	0.054	0.053
Conventional washing machine	0.301^{***}	0.052
Smart security camera	0.061	0.043
Robot vacuum cleaner	-0.126^{**}	0.043
Home router	0.072	0.043
Smart door lock	0.116^{*}	0.043
Connected printer	0.091^{*}	0.043
Smart smoke detector	0.244^{***}	0.043
Smart thermostat	0.434^{***}	0.043
Smart washing machine	0.232^{***}	0.043
Smartwatch	-0.221^{***}	0.043
WiFi solar inverter	0.469^{***}	0.043
Country *(Ref: Spain)*		
CountryFrance	-0.041	0.046
CountryGermany	0.092	0.046
CountryNetherlands	0.086	0.046
CountryPoland	-0.141^{***}	0.046
Device Experience		
Device category experience	0.080^{**}	0.024
Country:Smartness *(Ref: Poland)*		
Spain:Smartness	-0.049	0.045
France:Smartness	-0.071	0.045
Germany:Smartness	-0.085^{*}	0.045
Netherlands:Smartness	-0.122^{**}	0.045
AIC	3477.401	
BIC	3645.336	
Num. observations	2974	
Num. groups: Participant	993	
Conditional R^2	0.464	
Marginal R^2	0.166	

$^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$

Table 4: Regression model predicting expected device lifetime in the vignettes with Device Type, Country, respondents' Experience with the Device Category, and an Interaction between Country and the device's Smartness. "*Ref*" = Reference level. The outcome variable was log-transformed, and coefficients were exponentiated to denote an average increase or decrease in expected device lifetime, holding all other factors constant. Standard errors are not exponentiated.