Balancing Security and Longevity: Benefits of Modular IoT Infrastructure

Maxwell Keleher
Carleton University
Ottawa, Ontario, Canada
maxwellkeleher@cmail.carleton.ca

David Barrera
Carleton University
Ottawa, Ontario, Canada
davidbarrera@cunet.carleton.ca

Sonia Chiasson
Carleton University
Ottawa, Ontario, Canada
chiasson@scs.carleton.ca

Abstract

IoT device disposal involves all of the challenges associated with disposal of non-IoT devices, and introduces the additional challenge of purging sensitive data from the IoT components. These challenges push IoT device owners to make decisions with negative environmental, security, and privacy consequences. This paper investigates the extent to which security and privacy play a role in users' decisions to retire home IoT devices. Through an online questionnaire administered to 195 users, we seek to understand motivations and behaviours surrounding disposal of IoT devices. We find that security is not a direct motivator for owners to cease using IoT devices of all types; in many cases loss of functionality is a greater motivator to dispose of a device. We argue that a new modular security paradigm can allow both increased security for users and longer lasting devices.

Keywords

IoT, Usable Security, Longevity, Modular Design

ACM Reference Format:
Maxwell Keleher, David Barrera, and Sonia Chiasson. 2024. Balancing Security and Longevity: Benefits of Modular IoT Infrastructure. In *New Security Paradigms Workshop (NSPW '24), September 16–19, 2024, Bedford, PA, USA.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3703465.3703468

1 Introduction

Would you be comfortable using an Internet of Things (IoT) device which has a security vulnerability? If not, what would you do with the vulnerable device? As the proliferation of IoT devices continues, more users are increasingly faced with this dilemma. Other users remain unaware that the lack of vendor support can mean that some vulnerabilities will never be patched.

Unfortunately, the ubiquity of IoT devices has significantly contributed to e-waste production [35]. The devices that comprise IoT networks are often made non-operational by software updates which break functionality and may not be manufactured in a way that facilitates their repair when they break [48, 57]. It is currently unclear whether security and privacy concerns are causing IoT device owners to dispose of their devices. It is also unknown whether security and privacy factor into how IoT device owners dispose of their IoT devices.

NSPW '24, September 16–19, 2024, Bedford, PA, USA

ACM ISBN 979-8-4007-1128-2/24/09
https://doi.org/10.1145/3703465.3703468

In Canada alone, e-waste has tripled over the past two decades, and by 2030 it is estimated that Canada will generate over one million tonnes of e-waste annually [23]. IoT devices present a problem as they involve components necessary for some physical functionality (e.g., smart lights or smart kitchen appliances) and computing hardware to afford the digital functionality and connectivity. If poorly designed, an issue with the computing hardware might arbitrarily disable the physical functionality. This could lead to disposal of devices which are capable of performing the primary functionality, but are considered damaged or broken because they have lost the added IoT functionality. On the other hand, software issues or loss of server side support could render perfectly functional products inoperable. For example, Amazon announced they will "brick" the business version of their Astro robot only 10 months after making it available [45]. Similarly, Spotify will turn their Car Thing into e-waste after only 2 years of availability [7]. We should not dismiss IoT outright because of these issues; rather we should strive to reduce IoT's impact on e-waste production so that we can benefit from the positive effects that connected devices bring.

Adding internet connectivity to more products increases the number of devices in one's home that are vulnerable to security attacks or privacy violations. Many IoT device attacks, such as Mirai [3], are possible due to the unfortunate reality that IoT devices are not typically produced with security as a key concern. Security strategies such a firewalls can mitigate some risks but they are often avoided or misused due to usability issues [55]. Because IoT devices are often marketed as seamlessly integrating into a user's network, it is difficult to believe that users would adopt practices which introduce friction to the operation of their devices, even if those practices could extend the devices' lifespan. Ostensibly, IoT devices must be made reasonably secure to ensure that they are used for their entire potential lifespan.

Currently, there does not seem to be any research exploring IoT device owner attitudes and behaviours that might contribute to disposal of devices which are still functional nor exploring how they are disposing of their devices. This also means that it is unclear to what degree, if any, security and privacy concerns motivate IoT device owners to stop using their devices. When they dispose of IoT devices, are they adopting sustainable practices such as repurposing or recycling? Do IoT device owners take action to protect their security and privacy when disposing of their device?

In this paper, we are interested in understanding: *How do security and privacy relate to IoT device longevity?* Understanding this relationship between security, privacy, and longevity is critical to guiding the efforts of security and privacy experts in extending IoT device longevity. Without a clear understanding of how these

aspects relate, we risk focusing on security issues which do not extend device longevity or inadvertently contributing to a motivation for owners to dispose of their device.

In addressing this research objective, we developed a questionnaire and conducted an online study with 195 participants. We captured participants' expectations of IoT device longevity, and what they do with IoT devices when they stop using them. Based on the results of this questionnaire, we examine how security relates to device functionality, which was a significant motivator for participants to dispose of their IoT devices. To extend IoT device longevity and to maintain the security of IoT devices over their entire lifespan, we advocate for a new security paradigm which prioritizes modularity.

2 Background

2.1 Key Terminology

In our paper, we define and adopt the following terms:

Internet of Things. The Internet of Things (IoT) refers to a collection of digital devices which communicate data to each other over the internet or other wireless connections. The devices on such networks can be IoT devices or more powerful computing devices. Computing devices may also be used to control connected IoT devices.

IoT Device. An IoT device features physical and digital functionality, typically with the digital functionality supporting a primary, physical functionality. An IoT device should also leverage connectivity, both with other IoT devices and with computing devices broadly. Examples of IoT devices include smart lights, digital assistants (i.e. Amazon Echo or Google Home), smart TVs, and smart appliances. We do not consider general purpose computing devices such as computers, tablets, or smartphones to be IoT devices. For this paper, we are focused on consumer IoT devices and *not* enterprise or industrial-grade devices.

Retirement. We use the term retirement to refer to the phase in device ownership when the owner stops using the device. While they may be decommissioning the device from whichever purpose it served in their own life, they may give away the device or sell it to someone else. The owner might also go through the steps to properly recycle their IoT device, or might simply throw it into the garbage.

End of life. We refer to end of life as the point at which a device can no longer be used. Repairing damage, re-purposing a device, or giving it to another user could delay its end of life. Additionally, devices which reach end of life might be able to donate parts to repair other devices, but they are not usable on their own.

2.2 Security and Privacy Perceptions of IoT Devices

Generally, users' mental models and threat models of IoT devices seem to be incorrect or incomplete [1, 58]. IoT owners without technical backgrounds tend not to develop security and privacy concerns until after they have already purchased and used the devices [15]. This could result in waste as participants might become uncomfortable continuing to use IoT device about which they have security concerns. Even when participants express concerns about security and privacy, they do not tend to take any action to address their concerns [24].

Many of the concerns expressed by concerned users relate to how IoT devices collect information, and how the data is used after collection [19, 33]. Some of the security and privacy concerns with IoT are regarding the actions of the vendors, rather than the behaviours of the devices [15, 34]. Curiously, primary users of IoT devices seem less likely to have security and privacy concerns than "bystanders", others who interact with the device [2, 56, 59]. Moreover, bystanders seem to be more concerned about IoT devices than other computing devices, even though computing devices tend to be more capable than IoT devices [56].

2.3 IoT Longevity Expectations

How long are devices expected to last? On the surface, this question may seem easy to answer, but it is difficult to find authoritative studies or data on the topic. There are many different sub-types of devices within the designation of IoT, and there appear to be disparities in the expected longevity of these sub-types. For example, one would likely expect a large kitchen appliance such as a refrigerator or oven to outlast a light bulb.

In 2004, Tim Cooper [14] surveyed households about the expected lifespan of various household items. The mean responses for "reasonable" electric cooker or refrigerator lifespans was twice as long as the mean response for small work or personal care appliances. Over half of the survey respondents were dissatisfied with the lifespan of their small appliances compared to the roughly 35% who were dissatisfied with kitchen appliances. Moreover, only 5% of respondents thought it would be reasonable for small appliances to last more than 15 years [14]. If people apply similar logic to IoT devices, the expected longevity of smart kitchen appliances should generally be longer than smaller, cheaper IoT devices. When considering expected longevity, it is important to recognize that consumer expectations differ based on the type of device.

Expected longevity is made more complex because some IoT devices fundamentally change even the basic functionality of the device. Modern LED light-bulbs, including smart bulbs such as Philips Hue[1], claim to last an order of magnitude longer than traditional, incandescent light bulbs[2]. Smart lights are relatively unique among IoT devices both because they take advantage of a technology that provides a legitimate improvement over previous non-IoT versions of the object, and because the culture of the product field involves disclosing average lifespans. Consequently, consumers might expect certain IoT device sub-types, such as smart lights, to last longer than non-IoT objects. Despite these nuances stemming from the specific functionality or modality of different IoT devices, most IoT devices fit into generic product life cycle models.

Several researchers have used cyclical timelines to describe how devices are produced, used, decommissioned, and recommissioned. Both Garcia-Morchon et al. and Rahman et al. frame IoT device lifespans as cycles: devices are installed and commissioned before

[1] https://www.philips-hue.com
[2] https://www.bulbs.com/learning/arl.aspx

entering a sub-cycle of operating and updating before being decommissioned and possibly recommissioned for some new context [20, 39]. Maintenance might be performed locally to the device or could involve remote changes made to the back-end infrastructure supporting the device. In these cycles, reaching end-of-life does not mean that a device becomes trash, rather it no longer serves a purpose for the current owner and can be recommissioned by another. Bertino describes a complementary IoT Security Life Cycle comprised of a monitoring phase, mirroring the operational phase of the life cycle models, the diagnostic phase, mirroring with the decommissioning or maintenance phases, and the reaction and repair phase, mirroring the recommissioning phase [8]. Critically, these are generic, perhaps even aspirational, models that do not necessarily represent the current user behaviours.

Vendors cannot provide software features and security support indefinitely, as support tends to be viewed as an operational expense (and competes with sale of new devices). For this reason, vendors will nudge consumers to replace a device once support is no longer profitable. There are also technical challenges in supporting significantly older devices, such as retaining developer expertise and tooling [9]. If these challenges remain unaddressed, it is difficult to see a path toward long lasting, secure IoT devices.

In summary, an IoT device should last until it is no longer feasible for it to be recommissioned, but the exact point at which this determination is made will vary from device to device. Embedded, rechargeable batteries, common in wireless IoT devices, have a limited number of charge/discharge cycles and, though they are theoretically replaceable, it is often easier to replace the entire device [31]. Non-volatile flash memory also has a finite number of write cycles after which the chip must be replaced, although this repair requires specialized equipment. In terms of software, there may be a point at which there is no longer support to recover from a security vulnerability, or some core functionality may break beyond the technical ability for a vendor to repair it.

2.4 Premature Retirement of IoT Devices

A premature retirement is when someone retires their device before it has reached end of life. Consumers' behaviours contributing to premature IoT device retirement are relatively understudied. We were not able to find any work which investigates users' perceptions or mental models of IoT longevity, nor any studies about owners' motivations when retiring IoT devices which could still be used. However, we found some studies which explore related topics or issues. In research about general product lifespans, the product owner's behaviour unsurprisingly plays a significant role in length of the product's lifespan [25, 46]. Critically, product retirement decisions are not always rational, and often relate to social or emotional values [46, 53]. There have been studies about retirement and repair behaviours of digital devices, but not IoT specifically. Some people retain digital devices for sentimental or aesthetic reasons, but eventually they throw those devices away [50]. Owners also seem hesitant to repair their devices, especially themselves, since they consider device repair expensive or overly difficult [29, 38, 43].

Many IoT devices are designed in such a way that repair is not feasible [48]. When users are unable to repair or replace parts on IoT devices, they become responsible for properly recycling the device [26]. These design decisions that de-emphasize repair and maintenance likely contribute to the consumer perceptions that they cannot repair their IoT devices [38].

IoT devices include digital functionality and require long-term software support (often necessary to maintain compatibility with evolving server-side infrastructure) in order to remain functional. Older devices are often unable, seemingly artificially, to use newer applications, or might require that users possess newer devices to add newer software to older devices [22]. Moreover, otherwise functional IoT devices might become "broken" due to lack of software updates [27]. This digital infrastructure might also support IoT ecosystems to connect devices. Some IoT devices only function when part of their manufacturers' ecosystem. If disconnected from the eco-system, the devices could become effectively non-functional or lose significant aspects of their functionality.

A significant factor in IoT device decommissioning is the issue of product obsolescence which can be the result of several factors. Functional obsolescence significantly predates IoT devices and refers to cases where advancements in technology cause consumers to lose interest in older products [32, 40]. An empirical analysis of planned obsolescence in the textbook market found that increased competition from the used market contributes to shorter textbook revision cycles [28]. IoT device vendors might practice planned obsolescence by adopting practices such as fast fashion or marketing strategies, which encourage device replacement, or limiting maintenance services or part availability to prevent device repair [18, 42, 47].

Beyond individual behaviours, there are larger cultural factors which contribute to the poor longevity of IoT devices. Several researchers contend that the current linear economic structure encourages one-way production pipelines of IoT devices which go straight into the landfill once retired from use [5, 6, 9, 36, 48, 52]. That is not to say that we can maintain IoT devices indefinitely. Bradley and Barrera [9] acknowledge that IoT companies cannot offer software updates indefinitely, but that lack of updates could make unsupported IoT devices vulnerable to security and privacy attacks. Privacy and security are also key considerations when thinking about device decommissioning. IoT devices can collect significant amounts of information about users which can introduce risks if devices are reused without purging personal data [4, 57]. To facilitate safe reuse of IoT devices, there must be mechanisms for devices to be sanitized before they are reused or recycled. Nothing will last forever, so it is critical that we find compromises which balance sustainability and the reality of building and maintaining IoT devices.

2.5 Extending IoT Longevity

There are several suggested approaches to extend the secure operating period for IoT devices. Bradley and Barrera propose a new software stack which supports software updates for IoT devices once the vendor cannot [9]. Others have proposed solutions which seek to extend the functional life time of the devices. Khalid et al. seek to improve the energy efficiency of IoT devices to extend the life of rechargeable batteries [31]. ONiO is a company which seeks to develop IoT devices which completely avoid batteries by leveraging energy harvesting sensors (e.g., solar energy harvesting or

piezoelectric energy harvesting)[3]. These approaches are critical to reducing waste. All digital technology requires some form of power and finding efficient and sustainable ways of providing power can lessen the environmental consequences.

Bridgens et al. consider the longevity of a devices outward-facing materials rather than the digital components [10]. They propose that products should "age gracefully" to maintain user long-term user satisfaction and, in a user study comparing phone case materials, found that participants were quite dissatisfied with plastic as a material after it had aged. It is important that IoT devices with digital components that last a long time also consider their aesthetic attributes. If the appearance of physical touch points of an IoT device degrade over time, consumers might discard it despite it remaining functional. We consider this type of issue to be one that is more readily apparent when the problem is framed as a need to reduce waste versus a need to extend longevity.

Another solution space discussed in the literature is the proposal of holistic models or frameworks to shift the process by which products are designed. The Design 4 Conservation model [5, 6] provides a toolkit for designers so that they consider conservation throughout all phases of their design process. Similarly, Moreno et al. present a conceptual framework for adopting circular design strategies that reduce e-waste and promote reuse [36]. In 2023, Valušytė also recommended design strategies which can fit within the constraints present in circular economies [52]. Stead et al. call for a reframing of IoT devices as "spimes", which they describe as a move away from the disposable nature of IoT devices towards a "cyclical, ongoing, and sustainable approach " [48].

All of these proposals rely on designers shifting their practice. While this is certainly easier said than done, the success of frameworks such as Privacy by Design [12] illustrates the influence designers have over technology landscapes. Moreover, we believe that these proposals recognize that extending device lifespan alone will not address the increase in e-waste.

2.6 Security and Privacy Risks of Retired Devices

Data security and privacy is a known issue for e-waste disposal. Discarded hardware, such as routers or hard drives, can contain confidential information which is recoverable if the devices were not properly sanitized before disposal [11, 21, 49]. At a minimum, a discarded IoT device could expose an owner's network parameters and credentials. More sophisticated IoT devices might collect behavioural data about the owner which could be recovered after the device has been discarded. Additionally, IoT devices might collect user data without explicit consent and it may be difficult to determine and access the location where data is stored [44].

Unfortunately, many devices which are resold or discarded still have confidential information on them once they leave the original owner's possession. Studies of discarded devices show that many devices are not properly sanitized before disposal [11, 21, 30, 49]. When sanitizing their devices, users tend to rely on factory resetting their devices and some rely on manually deleting information [13]. A study about how second-hand device buyers react to finding data left on the device showed while many buyers would delete remnant data, some would keep the sensitive data perhaps notifying the seller or reporting to authorities if the device contained illegal content [37]. To facilitate secure reuse of devices, it is critical that reliable sanitization strategies are available on any device and that those sanitization strategies are usable for all users. Fortunately, there are known methods for secure deletion of stored data [41], however, to our knowledge, these are not yet common especially on lower-end devices.

[3]https://www.onio.com/article/batteryless-iot-why-it-matters.html

Table 1: Demographics for the participants included in the analysis (n=195).

		Count	Percent
Gender	Women	104	53%
	Non-binary	6	3%
	Men	83	43%
	Prefer not to say	2	1%
Country of Residence	Canada	143	73%
	USA	52	27%
Experience with technology	Yes	56	29%
	No	139	71%
Age	Median (years)	35	

3 Study Methods

In reviewing the existing literature which investigates the relationship between device longevity and security and privacy, we noticed that there was no work which detailed end-users' perceptions of IoT devices and behaviours related to retiring their IoT devices prematurely. To determine the relationship between security, privacy, and longevity, we needed to first answer two research questions about longevity expectations and retirement of IoT devices:

RQa What are end-users' expectations of IoT device longevity?
RQb What motivates end-users to retire their IoT devices?

In this section, we explain our process for developing our questionnaire, the inclusion criteria for our participants, and our recruitment approach. The study was reviewed and cleared by our university's institutional review board (IRB).

3.1 Participants and Recruitment

Through Prolific[4], we recruited participants who were over 18, lived in North America, and either owned or had owned an IoT device. We used Prolific's built-in filtering capabilities to target eligible participants.

We initially obtained 200 completed submissions through Prolific. The mean time to complete the questionnaire was 588 seconds. During data cleaning, we removed five submissions where the participants gave nonsensical responses, or seemed to have rushed through the questionnaire (providing the same answer for almost every question) or completed the questionnaire faster than one standard deviation from the mean completion time (faster than 231 seconds). In Table 1, we present the demographic information of the

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

195 participants included for analysis. Due to limitations in the pre-screening options, we are only able to ensure that participants have at one point owned or currently own an IoT device and not that they have previously disposed of a device. Given that we are not doing any inferential statistics, this sample gives us a 95% confidence interval with a margin of error of approximately +/- 7%.

3.2 Questionnaire Design

We developed a questionnaire to understand expectations of IoT device longevity, and the role of security and privacy in users' decisions to retire IoT devices. The full questionnaire can be found in Appendix A. Previous studies [14, 29] have used questionnaires to investigate the expected lifespan of computing device or household objects. We use these questionnaires as a starting point to build our own. The first step for developing our questionnaire was to determine the categories of IoT devices to include in the questions.

3.2.1 Device Categories. The expected lifespan of an object or device can vary based on many characteristics, e.g., its purpose, construction, or form factor. Consequently, previous studies on longevity expectations have asked about specific categories of devices or appliances.

As referenced above, Prolific offers self-reported demographics for filtering participants, including a section of "internet enabled technologies". Our initial set of IoT device categories was taken from Prolific's list.

While this list is quite exhaustive, it appeared to be unnecessarily specific in some areas (e.g., the smart water sprinklers), and rather vague in others (e.g., by grouping all kitchen appliances into a single category). To improve the clarity of the questionnaire, and reduce the demand on participants' time, we condensed the list of IoT device categories from ten to the seven categories described in Table 2. For each category, we formed an IoT and Non-IoT pair, by identifying the closest corresponding non-IoT device.

3.2.2 Definitions. To ensure that all participants had a common understanding, we provided participants with the following definitions. These were visible throughout the questionnaire.

IoT: Internet of Things refers to a collection of digital devices which communicate data to each other over the internet or other wireless connections.

IoT device: An IoT device is something which has internet-enabled features and/or can connect to other devices (e.g., smart refrigerators, smart lights, smart thermostats). We do not consider computers or phones to be IoT devices.

Non-IoT device: A non-IoT device is one which is not connected to the internet. They are the original version of the device or appliance that existed before an IoT version. Sometimes these are referred to as "dumb devices" in contrast to the newer "smart" devices (e.g., a "dumb" fridge vs a "smart" fridge).

3.2.3 Longevity Expectations. In our initial literature exploration, we found no research investigating participants' expectation of IoT device longevity. To understand participants' attitudes and behaviours towards retiring devices, and the influence of security and privacy, we first needed to determine their expectations for how long IoT devices should last. In our questionnaire, we asked participants to indicate how many years they expect the IoT and non-IoT versions of each device type to last and how long they expected parts to be available for repairing each.

3.2.4 Retirement Motivations and Behaviours. Next, we wanted to understand participants' motivations for retiring their devices and their behaviours when retiring devices they no longer use. We asked participants to rank eight motivations for retiring their IoT devices. The first six motivations are based on a questionnaire produced by Jaeger-Erben et al. [29]. To provide insight into the relative importance of privacy and security as motivations, we added options relating to device security and the personal data collection. We included an optional textbox where participants could describe any other motivations. Additionally, we included an open-ended question asking participants to briefly describe what they did with the last IoT device they retired.

3.2.5 Security and Privacy. We sought to understand how security and privacy factor into participants' IoT device longevity expectation and retirement behaviours. We first ask participants to provide the number of years that they expect each type of device to receive software updates addressing functionality and updates addressing security vulnerabilities. Responses to these questions will complement the questions about availability of parts to repair IoT devices by giving insight into the expected longevity of IoT device software.

Later in the questionnaire, we use Likert-style questions to evaluate how participants compare older and newer IoT devices with respect to security and privacy. These questions could capture attitudes which might lead owners to prematurely retire an IoT device so that they can own the most secure and privacy preserving option. We also ask participants to compare the security and privacy of IoT and non-IoT devices. This question complements the questions on expectations of longevity and availability of repair parts.

3.3 Analysis

We primarily use descriptive statistics and graphs to analyze the questionnaire data. Detailed comparison between categories of devices was not the intention of this current analysis, so we do not include inferential statistics. We analyzed rankings by determining the number of participants who ranked each motivation at each level. Similarly, we determined how many participants reported practising each of the e-waste reducing retirement behaviours per IoT device types. For the Likert questions about security and privacy, we reviewed the distribution of participants' responses.

We used inductive qualitative analysis to analyze responses to the optional open-ended questions about (i) motivations and (ii) behaviours relating to retiring a device (available in Section A of the questionnaire in Appendix A). First, one of the researchers applied open codes to the responses. Next, the research team reviewed the assigned codes and grouped those that were similar. The final codebook is presented in Tables 4 and 6.

3.4 Study Limitations

29% of our participants self-identified as having some technological expertise, which might be a higher ratio of technology experts than the broader population. This could mean that our results reflect a more sophisticated understanding of IoT devices than the broader

Table 2: The seven device categories used in the questionnaire, each row identifies the corresponding IoT and non-IoT device pair.

IoT Device		Non-IoT Device	
Types	**Examples**	**Types**	**Examples**
Smart TVs		TVs	
Smart monitoring	baby camera/monitor, Security camera	Monitoring	baby camera/monitor, Security camera
Smart emergency alerts	smart smoke alarms, smart flood detector, smart CO2 detector, smart power outage detector	Emergency alerts	smoke alarms, flood detector, CO2 detector, power outage detector
Large smart appliances	smart fridge, smart oven, smart washer, smart dryer	Large appliances	fridge, oven, washer, dryer
Small smart appliances	smart kettle, smart scales, smart vacuum cleaner	Small appliances	kettle, scales, vacuum cleaner
Smart lights		Light bulbs	
Home automation	smart thermostat, smart plugs, smart lock and/or doorbell, smart water sprinkler/irrigation controllers	Home fixtures	thermostat, wall outlets, door lock and/or doorbell, water sprinkler/irrigation controllers

population. Also, we did not explicitly ask about knowledge of security and privacy vulnerabilities to avoid priming. None of the participants mentioned vulnerabilities in the open-ended questions.

Additionally, we did not specifically collect information on participants' socioeconomic backgrounds. It is unclear how socioeconomic status may influence likelihood to repair or maintain devices to extend usage. It would be valuable for future work to investigate whether a causal relationship exists between socioeconomic status and device retirement motivations and behaviours.

Due to the lack of existing research and knowledge, we opted to pursue a questionnaire to ascertain a high level understanding of the relationship between security, privacy, and longevity. We were unable to follow up with participants for further details about their attitudes and behaviours, but are able to identify common patterns of behaviour due to the larger sample size.

Several of the questions were presented broadly in our questionnaire and did not distinguish between types of IoT devices. We did this to avoid an overly long questionnaire which placed a significant time burden on participants. It would be valuable to follow up on our findings by exploring differences in security attitudes based on the category of IoT device.

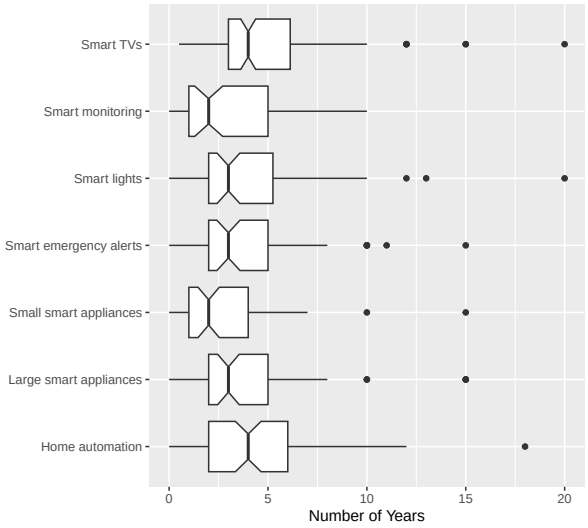

Figure 1: Length of time participants have owned a device in each of the IoT device categories. If participants owned multiple devices of a type, they were asked to provide the longest ownership duration.

4 Study Results

In this section, we report participants' responses to our questionnaire and review how these results address our two research questions about longevity expectations and IoT device retirement.

4.1 Device Ownership

We asked participants how long they had owned each of their IoT devices (see Figure 1). The median duration of ownership for every IoT device category was less than five years. Moreover, only eight participants reported owning any IoT device for longer than 12.5 years. Participants generally seemed to have owned smart monitoring and small smart appliances for a slightly shorter amount of time than devices from other categories.

4.2 Longevity Expectations

We asked several questions to understand participants' expectations of IoT device longevity. We asked about their overall expectation of how long each type of IoT device will last, how long they expect each type of device to have parts available so that it can be repaired, and how long they expect the device to receive software updates.

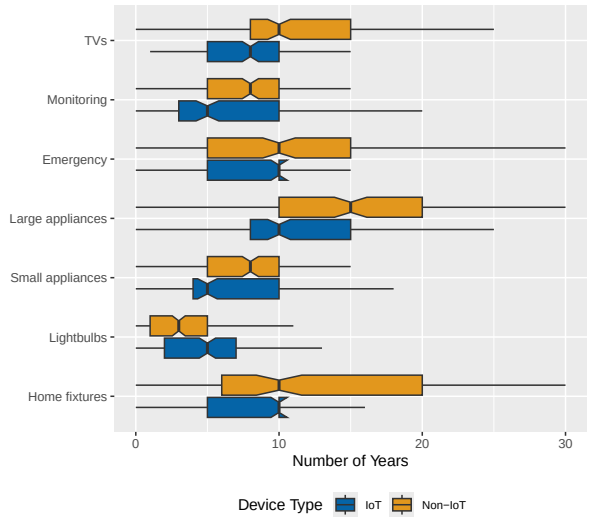

Figure 2: Expected lifespan (in years) for each category of IoT and non-IoT device.

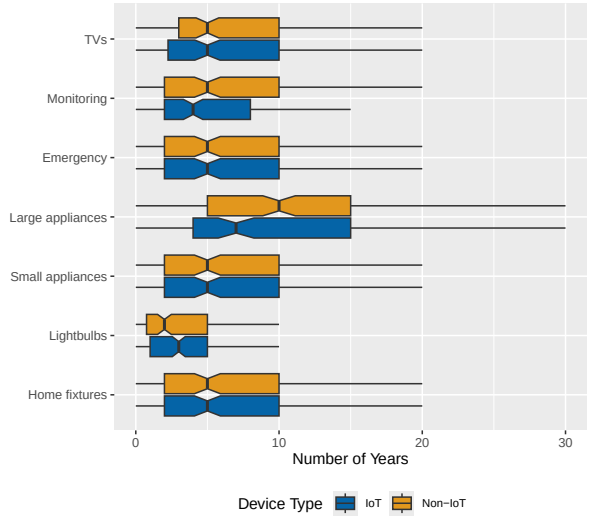

Figure 3: Expected availability of parts (in years) so that devices can be repaired, for each category and type of device.

In Figure 2, we report participants' expectations of how long IoT and non-IoT devices of each category will last. In most cases, participants expected that IoT devices would have a shorter lifespan than non-IoT devices. The only exception was that participants expected IoT lightbulbs to last longer than non-IoT lightbulbs. Considering the seven IoT device categories, participants expected that large appliances to last longest.

We asked participants how long they expected parts to be available so that they could repair their devices. As shown in Figure 3, the medians were 10 years or less for all categories, and participants' expectations tended to be similar for the IoT and non-IoT devices of each category. The expected availability of repair parts was shortest for light bulbs and longest for large appliances. Interestingly, they expected the repair parts to be available for a shorter duration than the devices' overall expected lifespan.

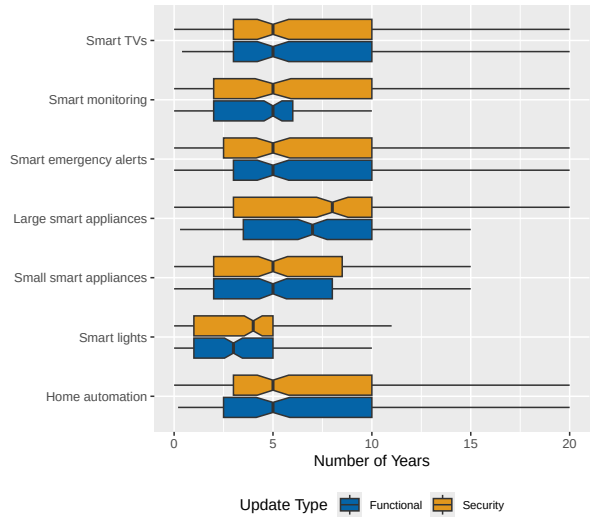

Figure 4: Expectations time frame for software updates relating to functionality and software updates addressing security vulnerabilities.

4.3 Software Update Expectations

In Figure 4, we report the number of years participants expected to receive functional updates and security updates. Generally, participants had similar expectations regarding both functional and security updates for each pair of devices.

Participants generally expected to receive functional and security software updates for approximately five years. The shortest expectation was for smart lights would, which participants expected to receive functional updates for approximately three years. The longest expectation was that large smart appliances would receive security updates for over 7.5 years.

4.4 Motivations to Retire an IoT Device

Participants ranked the relative importance of eight different motivations for retiring their IoT devices, where 1 = most important and 8 = least important. We report the number of participants who selected each rank per motivation in Table 3. There seemed to be very little consensus among participants other than agreement on the importance of device functionality; over half of participants ranked having a non-functional device as the most important motivation for retiring an IoT device. After lack of functionality, participants ranked wanting a new model and receiving a special offer to obtain a new device as fairly important. Most participants ranked feeling that the device was insecure or that it collected personal information as relatively unimportant.

Participants could provide additional details in an open textbox; we present the extra motivations which participants expressed in

Table 3: Number of participants (n=195) who ranked each motivation to retire IoT devices at each level, where Rank 1 is most important and Rank 8 is least important. Darker cell colourings indicate that a greater number of participants ranked the motivation at the corresponding importance ranking. Cells with counts are grouped into 10 ranges of 10% of the largest count (i.e., the darkest colour represents values which are at least 90% of the largest count and the lightest corresponds to those that are less than 10% of the largest count.)

	Rank 1	Rank 2	Rank 3	Rank 4	Rank 5	Rank 6	Rank 7	Rank 8	Mean	Median
The device did not work anymore	118	16	13	15	10	9	5	9	2.4	1
I wanted to have a new model	21	43	28	26	21	20	19	17	4.0	4
Because I found a special offer for a new device	11	37	37	36	36	22	10	6	4.0	4
Because I felt the device was insecure	15	29	21	20	18	30	36	26	4.8	5
I felt that I had used my last device long enough	4	21	27	31	24	29	32	27	5.0	5
I found a model with a more attractive design	6	19	20	21	30	36	36	27	5.2	6
Because I felt that device was collecting personal information	8	17	35	20	20	19	33	43	5.2	5
A new device gives me joy	12	13	14	26	36	30	24	40	5.3	5

Table 4: Additional motivations to retire IoT devices (26 participants responded out of 195)

Motivation to Retire IoT Device	Count
Device was broken (unspecified component)	10
Loss of Software Functionality	9
Loss of Hardware Functionality	2
Device did not fit with lifestyle	4
Concern about security vulnerability	1

Table 4. A common additional motivation for IoT device retirement was due to some issue with its software. Participants mentioned retiring their device because it was not compatible with other IoT devices they owned, or because it no longer received new features through software updates. Other participants mentioned issues such as low usage or poor cost effectiveness. Only one participant, P139, stated that they felt there were "significant security flaws" with their IoT device which motivated them to retire it.

4.5 E-waste Reducing Behaviours

We asked participants about whether they had undertaken three different types of behaviours which might reduce e-waste: giving away a device they were retiring, selling a device they were retiring, or purchasing a device second hand. 75 participants (38%) responded that they had practised at least one of the e-waste reducing behaviours with at least one of the IoT device categories. In Table 5, we break down how many participants practised each behaviour per category of device. Participants most frequently practised any of these behaviours with smart TVs. Generally, selling used IoT devices was most commonly reported among participants.

Table 5: Number participants who reported practising behaviours which reduce e-waste per IoT device category (n=195).

	Gave Away	Sold	Bought Second-hand
Smart TVs	14	22	12
Smart monitoring	4	13	7
Smart emergency alerts	3	2	3
Large smart appliances	5	2	6
Small smart appliances	5	11	4
Smart lights	3	11	10
Home automation	3	7	7

Table 6: What participants did with IoT devices once they were no longer using them (178 participants responded out of 195).

Theme	Retirement Behaviours	Count
Discarded	Threw in the garbage	37
	Unspecified disposal	13
	Recycled	22
Second life	Gave device away (possibly to stranger)	9
	Gave to family or friend	17
	Donated to thrift store	3
	Sold	19
Kept	Stored	25

4.6 IoT Device Retirement Behaviours

178 participants responded to an open ended question describing specifically what they had done with the last device they had stopped using. We used inductive qualitative analysis to look for

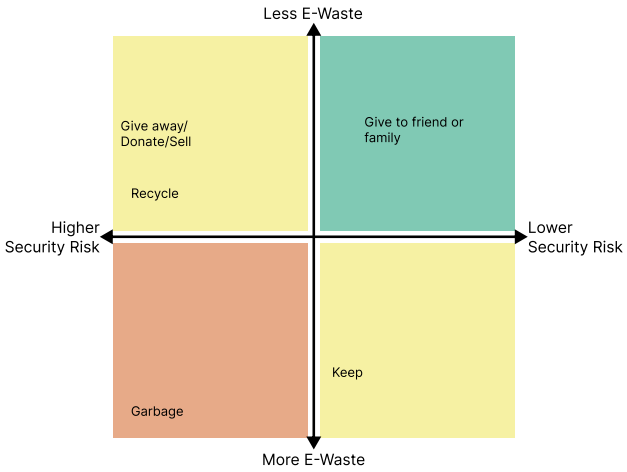

Figure 5: Simplified visualization broadly depicting the relationship between security risks and level of e-waste generation. Risks may be less when devices do not contain sensitive information.

common behaviours in participants' responses, which we then grouped into three themes. Most did not specifically mention the type of device they had retired, but they described behaviours with varying impacts on e-waste, and security and privacy.

As shown in Table 6, the largest set of participants mentioned that they discarded the last IoT device they retired. 13 did not specify how they discarded the device, but 37 other participants explicitly stated that they threw it in the garbage. On the other hand, 22 participants mentioned recycling the device they were retiring. 10 participants in this theme mentioned that they brought their device to a designated recycling or e-waste collection spot. Three participants explicitly mentioned Best Buy (a North American chain of consumer electronics stores that provide bins for individuals to drop off e-waste for free) as the location to which they brought their devices for recycling.

27% of respondents described behaviours which might give the retired device a second life. Many participants talked about giving their device to friends or family, and some also mentioned giving away their device to strangers or donating it to a thrift store. Many participants also mentioned having sold their retired IoT device.

25 participants mentioned keeping a device which they no longer used. In most cases, it was unclear what motivated this behaviour (e.g., privacy concerns, lack of time, sentimental attachment). One mentioned keeping the device in a secure location and three others referenced plans to eventually donate or sell the device. The security, privacy, and longevity impacts of this behaviour are nebulous since owners will eventually need to dispose of their device in some way. An owner eventually throwing out a device they kept is likely no better than if they just threw out the device in the first place.

While keeping a device stored can appear less wasteful than immediately throwing it in the garbage there is a limit to how long IoT devices receive software support. So there is waste when a currently supported device goes unused in the sense that useful "supported time" is not used. Although kept devices might not be damaging the batteries through charge/discharge cycles, prolonged periods without charging can also degrade batteries.

Importantly, **none** of our participants mentioned taking any action to remove sensitive information from their device before they discarded, recycled, gave away, or sold the device.

In Figure 5, we provide a general visualization of participants' most common IoT device retirement behaviours. The figure is organized along two axes reflecting the amount of e-waste and the degree of security risk, generating four quadrants. We position the behaviours within these quadrants to give a relative approximation of their position and facilitate reflection. Ideally, we would encourage behaviours in the top right quadrant (in green) to reduce both e-waste and security risks, while discouraging behaviours in the bottom left (in orange) which have a high degree of e-waste and security risk.

4.7 Security and Privacy Attitudes

We first asked participants 5-point Likert questions whether they considered IoT or non-IoT devices to be more secure and more privacy preserving (see Figure 6). The majority of participants believed that non-IoT devices are more secure and privacy preserving.

Secondly, we asked participants whether they considered older or newer IoT devices to be more secure and more privacy preserving (see Figure 7). Responses were quite evenly distributed for the privacy question. However, the majority of participants consider newer IoT devices to be more secure than older IoT devices.

5 Discussion

In this section we address our research questions and discuss the implications of our findings. We begin by reviewing findings relating to the sub-questions since they provide contextual understanding about end-user attitudes and behaviours regarding the sustainability of IoT devices.

RQa: What are end-users' expectations of IoT device longevity? Participants indicated the longest expected lifespan for smart emergency alert devices, large smart appliances, and home automation devices. We briefly speculate why this may be. Emergency alert and home automation devices typically require initial setup but do not require frequent user interaction. If participants conceptualize a device as having some maximum number of uses, then it would be reasonable to expect devices which are used infrequently to reach their end of life slowly. Although monitoring devices are also used passively, these typically collect video and audio. Participants may consider an older IoT device with poor video quality to be obsolete, whereas an older moisture sensor for flood detection may be viewed as still sufficient.

RQb: What motivates end-users to retire their IoT devices? The fact that loss of functionality was the most important motivation indicates that end-users might not be prematurely retiring their devices. After all, we would not expect someone to use a non functional IoT device. If a device were to become non-functional, the only options available are to repair the device or to retire it. Owners perceive significant barriers preventing them from repairing their IoT devices, even those interested in repair [29, 38]. Unless participants are using their devices recklessly, an IoT device's durability is

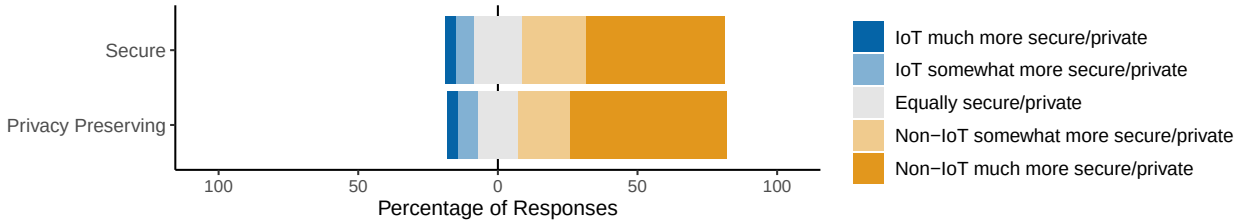

Figure 6: Responses to 5-point Likert questions about whether IoT or non-IoT devices are more secure and more privacy preserving.

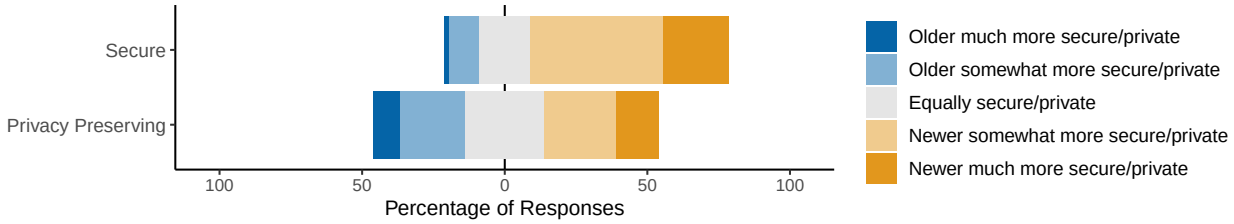

Figure 7: Responses to 5-point Likert questions about older or newer IoT devices are more secure and more privacy preserving.

determined by how vendors design and build them. Therefore, the onus is on the vendors to release more durable devices. It would also be important to improve the usability of repair options so that participants can repair their devices rather than throw them in the garbage. Right to Repair movements, which advocate for products owners to have access to the resources necessary to repair the products, are a critical to ensuring long lasting devices. There does not seem to be a consensus about the importance of the other motivations. It would appear that interest in newer models of IoT devices is more likely to be motivated by addition of new features or improved performance rather than aesthetic differences.

5.1 Role of Security and Privacy on Device Longevity

Our overarching research goal was to investigate: *How do security and privacy relate to IoT device longevity?* Concerns about IoT device security and privacy tended to be ranked as less important relative to other motivations. While device security did not rank highly as a motivation for retiring a device, we want to highlight that security has the potential to impact longevity indirectly. Exploited security vulnerabilities, which could be effectively invisible to a user, might degrade device performance or functionality. Additionally, we believe that extreme security measures which limit the available functionality of a device could unintentionally drive premature device retirement.

In terms of privacy, the lack of concern for data collection may be connected to participants expectations of IoT devices. Most devices collect personal data, such as location, for their automated functionality. So the collection of personal data might not be the issue, rather concerns might relate to who has access to the personal data. It is also possible that IoT device owners are generally less concerned about privacy since many IoT devices must collect personal data to function. By owning and using an IoT device, owners are likely prepared to give up some of their privacy.

Synthesizing these implications about security and privacy, it appears that security is has greater potential for impact on IoT device longevity than privacy. Since privacy ranked as relatively unimportant, efforts to improve device privacy seem unlikely to lengthen usage and ownership of IoT devices. Functionality was the most important motivator for participants to dispose of their devices and efforts to improve IoT device security should be mindful of that fact. Improved security, which defends the device's functionality, might have the knock-on effect of delaying the point at which the device owner retires the device due to poor functionality. However, over-zealous security measures risk influencing device owners to retire their device due to perceived loss of functionality. When working to improve device security, it is generally important not to compromise performance and functionality for security.

Some governments have enacted regulations which seek to mitigate the privacy and security risks presented by IoT devices. In the United States, there has been a program for IoT vendors to voluntarily provide cybersecurity labels for products [17], and the Children's Online Privacy Protection Rule (COPPA) aims to enforce proper data handling for products and services which are used by children [16]. Similarly, the UK enacted the Product Security and Telecommunications Infrastructure Act to mandate that IoT vendors follow basic security practices such as avoiding weak default credentials and providing ways to report vulnerabilities [51]. While these are important measures, they do not address the issues which drive IoT owners to prematurely retire their devices.

Participant behaviours when retiring their IoT devices also had varying privacy and security implications. There are two factors about retirement behaviours to consider: impact on e-waste accumulation and security and privacy risk. Many participants reported just throwing their device in the garbage. This behaviour is bad

from a sustainability perspective, since it generates e-waste, but, it also presents some risk to security and privacy. None of the participants described removing personal information from their devices before they disposed them. Therefore, an attacker could pull the data off of their device after they discard it. This same risk is present with recycling, but, recycling is better from a sustainable perspective (see Figure 5). Better still, from a sustainability perspective, are those who sold, donated, or gave away their devices. However, these possess the same risk of leaking personal information if proper care is not taken to remove personal data from IoT devices. Notably, some participants mentioned giving their device to friends or family. This behaviour might mitigate the security and privacy risk if the person giving away the IoT device is comfortable with their family accessing their personal data on the device.

Several participants referenced keeping their devices at home after they stopped using them; one even specifically referenced storing it in a secure location. We did not specifically ask about whether users might use their device again after temporarily retiring it, but the fact that several referenced giving their unused devices to others demonstrates that a device's lifespan does not necessarily end when its current user stops using it. This behaviour is notable since it does not immediately contribute to e-waste or expose the device owner to security and privacy risks. However, it is not possible for someone to store all of their retired devices indefinitely. Moreover, Thorp et al.'s study [50] indicates that device retention generally just delays disposal of the device into the trash.

Perhaps participants are retaining their retired devices until they have time to properly sanitize and recycle them. Holding onto an unused device may indicate that participants wish to properly recycle their devices and protect their security and privacy, but feel that they lack the skill, experience, or knowledge to act effectively. Bradley and Barrera [9] note that the cost of taking am IoT device to an appropriate recycling centre may exceed the cost of the device itself. Retaining retired devices may give people the chance to accumulate a critical mass of devices which justify the cost of transporting them all to a recycling centre.

5.2 Disposal Confusion

Several participants expressed confusion or, ostensibly, frustration with sustainable disposal methods. This difficulty in responsible waste disposal is not new and is not isolated to e-waste. In Canada, some municipalities and provinces offer apps or websites to help citizens understand how to dispose of their recyclable waste, typically called What Goes Where[5].

It is worth noting that some participants specifically referenced the places that they brought their devices for disposal. Some mentioned that they brought their devices to dedicated e-waste recycling centres. A few participants mentioned that they recycled their IoT devices at Best Buy. Deposit boxes have proven effective for increasing consumer recycling of plastic waste [54], so a similar model may help encourage others to recycle IoT devices they would otherwise throw away. Regardless of how IoT device recycling is facilitated, it is critical that both the usability and the information security of the process are prioritized.

6 Re-thinking the Role of Security and Privacy on Device Longevity

When a critical component in a device fails, the entire device is deemed to have failed (e.g., when the compressor in a refrigerator fails, the refrigerator can no longer keep food cold so it can no longer be used). A device's longevity is thus capped by the lifespan of its most fragile, load-bearing (critical), component. A failure in any of these essential components will likely be reported as "the device did not work anymore" (see Table 3), but only in extreme cases will all of the critical components fail simultaneously. Put differently, if a vendor wants to ensure a device lasts for 10 years or more, they need to ensure every critical component can actually remain functional for at least 10 years. If components can't be built to last this long (e.g., due to normal wear and tear), it will be necessary for these parts to be repairable/replaceable so that the device can remain functional for longer periods.

Devices with larger numbers of individual load-bearing components are less likely to last as long as those with fewer components. Participants in our study appeared to understand this logic (even if only intuitively) when comparing expected lifespans of IoT devices to their non-IoT counterparts (see Figure 2). In almost all cases, respondents felt that devices with IoT capabilities were less durable than those without IoT capabilities. Indeed, when IoT functionality is made critical to the overall device functionality, it will need to be supported and maintained for as long as the non-IoT components. In other words, IoT capabilities, when added to a device or object, add another piece of functionality that vendors need to support. Unfortunately, vendors do not typically support software for long periods of time or make repairs easy for end users, neither do customers expect them to according to our results, meaning that IoT functionality reduces the longevity of devices.

Software security and data privacy further complicate matters. Security-related code and functionality (e.g., cryptographic algorithms, encryption keys, TLS[6] certificates) often come with implicit or explicit expiration dates. Cryptographic key sizes tend to grow over time to protect against attackers with more computational power, and root certificate trust stores literally state the last day a certificate should be trusted to verify secure connections. Deploying security software intended to run for long periods of time on IoT devices without considering updates or replaceable software is thus likely to result in vulnerabilities in the medium/long term.

Users in our study did not consider security and privacy as load-bearing in any of the product categories. This is perhaps unsurprising, as security and privacy are usually not the user's primary task when operating IoT devices. Moreover, the lack of screens and status indicators make it difficult to determine system status at any given time, as well as what the software status, quality, or vulnerability is[7]. This implies that IoT device owners are unlikely to retire a vulnerable IoT device which has no other issues.

[5]For example, https://ovwrc.com/what-goes-where/, https://www.markham.ca/wps/portal/home/neighbourhood-services/recycling-garbage/what-goes-where/what-goes-where, and https://cavaouwebapp.recyc-quebec.gouv.qc.ca

[6]Transport Layer Security

[7]It would appear that in attempting to make things smart, designers have managed to ignore decades of research in user interface design https://www.nngroup.com/articles/visibility-system-status/.

While the continued use of vulnerable devices is positive in the sense that it does not directly contribute to premature device retirement (and therefore to e-waste generation), it is far from ideal from a security perspective; keeping a vulnerable device online could offer attackers access to the users' home network and personal/usage data (see Section 2.6). In addition, when exploited, vulnerabilities can impact device functionality, which is the main reason users retire devices. And finally, when users ultimately retire their devices, all personal information stored on the device needs to be protected. We argue that a fundamental shift is needed in the way we design and support devices to improve security, support users, and protect the environment from unnecessary waste.

6.1 The case for a new (modular) paradigm

When considering potential solutions to the security/longevity problem, our results suggest that focusing solely on security is unlikely to have a large effect on user behaviour. For example, if it became mandatory for IoT vendors to offer security patches for 10 years, and users diligently applied these patches, their devices would behave no differently than vulnerable devices that have not been compromised. In both cases, users would replace their devices when the functionality no longer satisfied their requirements, except the vendors in the former case will have incurred substantial costs to support the devices for such a long period. Indeed, it is difficult to see how placing emphasis on security above all else results in more sustainable outcomes.

In our discussions, *modularity* emerged as a promising direction to balance between security and longevity while empowering end users. We see modularity as a proactive solution in contrast to the reactive nature of repair. We were inspired by real-world companies making modular products that can be heavily customized, repaired, and even repurposed. To our knowledge, the most notable modern are examples the Framework laptops[8] and AIAIAI TMA-2 headphones[9]. Both of these companies believe in sustainability as a core tenet, and want to make it easy for users to extend their life of their products. Repairing a device focuses on preserving functionality, where as the above companies demonstrate that modularity can afford extension of a device's original capabilities.

The modular design philosophy offers several benefits from a sustainability standpoint. Customers have the ability to tailor the device to their specific needs which can reduce waste in terms of unused components or features. There is the obvious ease of repair should a component fail: simply purchase the individual component and easily swap it out[10]. Modularity also affords customers the opportunity to upgrade specific components, rather than purchase more expensive models of the device, should their context of use or needs change over time. Well designed modular devices make it trivial to switch components, which can empower users who might otherwise feel intimidated performing repairs.

How can modularity help in our case? We view modular design as an essential principle to follow throughout the various layers of device stack as described below. While implementing modularity at all layers has the obvious benefit of creating more ways to independently swap out components in both hardware and software, supporting modularity in at least one level can have substantial benefits over not doing so at all.

Modularity in hardware. General purpose desktop computers are built with standard interfaces for connecting peripherals and core components. CPUs, memory, and graphics cards can easily be removed from the motherboard and replaced, and USB serves as the standard interface for connecting peripherals. Modular IoT device hardware could enable user-repairable/user-upgradable devices much like general purpose computers. For this to be possible, standard connection interfaces (much like PCI or SATA on computers) are necessary. One can imagine a tiny removable "security card" that contains a trusted platform module for storing personal information and some recent cryptography-specific processing capabilities. It could also include enough flash storage to hold the few root certificates needed by the device. This card could be used across multiple devices and vendors, and be replaced when the on-board algorithms become outdated. Another benefit is that at disposal time, the user can remove and keep the security card to ensure their data is not accessed by the next device owner. Of course, the usual compatibility caveats apply: the industry would need to agree on a standard interface and vendors would need to accept that they might not earn revenue from this part of the business. Consider that this modularity need not be constrained within the digital components of the IoT device. The physical and digital components of an IoT device should be decoupled such that one could be reused if the other breaks beyond repair.

Modularity in firmware. Locking a device to a specific version or source of firmware inevitably results in abandoned support for that firmware. As discussed by Bradley and Barrera [9], allowing users to switch away from the vendor-provided firmware can open paths toward community (or even other vendor) support. For replaceable firmwares to be possible, vendors will need to give up on the idea that only they are authorized to provide updates. In practice, this requires some way for the user to switch to a new trusted firmware provider (for example, this could be done with a long press of a small internal button or some other physical signal). Automatic switching, as suggested by Bradley and Barrera could be abused by attackers. From a technical standpoint, modular firmwares require the underlying hardware to be sufficiently abstracted[11] such that reverse engineering is not required for every new device [9]. Hardware abstraction layers are already deployed outside of IoT, so more work is needed to bring those to the IoT domain.

Modularity in software. IoT device software is written in systems-level programming languages like C. Depending on the device, there may only be a small number of cryptographic libraries to choose from, and all except the built-in library could be incompatible with the device's codebase. More software engineering work is needed to offer better abstractions such that new libraries can be swapped to replace old or unsupported libraries without impacting user-facing functionality. The trade-offs here are that standard APIs can be

[8] https://frame.work/ca/en

[9] https://aiaiai.audio/headphones/tma-2-build-your-own/s02h02e02c02

[10] Anecdotally, our research uncovered many instances of online communities praising specific vendors or products (especially very old products) for their "repairability". In most cases, repairability is primarily due to modularity of components followed by availability of parts and accessible (as in easy to access) internal components

[11] Since IoT hardware tends to be custom made for specific hardware revisions, it would help a new developer to communicate with the hardware through a standard abstraction layer, rather than directly to the low-level hardware.

restrictive toward new features, but making the APIs too expressive can make implementation difficult or inconsistent. There is also an opportunity for modularity at the ecosystem level. This could avoid the problem were a loss of the server-side functionality effectively breaks an IoT device. It could also allow vendors to transfer some of the security responsibility. For example, a smaller vendor may opt to leverage a larger, more established ecosystem with reputation for strong security practices.

Security and privacy risks of modularity. Security, privacy, and e-waste are complex problems and we acknowledge that modularity will not inherently solve all issues. For example, modular storage would still involve the risk of confidential information being recovered after disposal. For this reason, when developing modular IoT devices, it will be critical to consider the security, privacy, and disposal implications of each new device. We expect the diversity of IoT devices will lead to an equivalent diversity of threat models for modular IoT, and each will need to be carefully considered.

6.2 Other avenues to explore

We recognize that modularity may not be the best or only solution in all cases. For example, it may not be financially feasible to implement modularity with devices like smart lights which have relatively little hardware compared to larger, more complex devices. In such cases, it is important to facilitate proper recycling to minimize e-waste.

Bradley and Barrera explain that device leasing is not a strong solution to longevity of consumer IoT devices, but that it is a reasonable approach when considering enterprise consumers [9]. Our survey targeted individuals who used IoT, but it would be valuable to understand enterprise device retirement motivations and behaviours as well as assess the impact of modularity. Given that enterprise consumers are more likely to leverage economies of scale, they are perhaps have greater incentive to buy into a modular paradigm to reduce waste. Moreover, enterprise customers might have longer and more involved relationships with vendors compared to individuals. A vendor might predict a better return on investment for investing in modularity if they expect to have a long-term relationship with their customers. Overall, enterprise IoT consumers are likely to have different perceptions and priorities with respect to device longevity which offers new opportunities for balancing security and longevity.

Even a modular IoT device will eventually reach a point where it can no longer feasibly be used. While proper recycling would be appropriate in such cases, there is also an opportunity to donate some of these devices for educational purposes. These devices could be taken apart so that people can learn about them. This would extend the utility of non-functional devices. Organizations (e.g., schools, libraries, community groups who host educational workshops) might maintain a public "wish list", visible to the community, of devices that they would like to receive. These organizations could use the non-functional devices to teach how the original items work or re-use components in creative building activities.

7 Conclusion

We note that especially in the case of modular hardware, our proposal herein does not do away with e-waste since we are now advocating for swapping out small printed circuit boards. What happens to the old boards? This is something that the community will need to consider: is it better to dispose of one or two SIM-card sized security cards over a 10 year period, followed by the disposal of the main device, or to dispose of the full device every five years? We will need quantify the environmental damage that each potential scenario could create, along with consideration for alternative uses for old modular hardware and recycling potential.

There are several aspects of the e-waste problem, such as the aforementioned quantification of environmental impact, which require collaboration with experts from outside the security community. While security and privacy experts can work to address factors leading to poor IoT device longevity, that is only a small piece of a larger problem. Within our own study, we found other factors contributing to e-waste. Behavioural issues, such as when a user considered a device so damaged that they cease using it. We also found systemic issues, such as how accessible and available device recycling deposit options are and how clearly appropriate disposal procedures are communicated to device owners. To maximize our impact, we as security and privacy experts must cross disciplinary boundaries and work with experts in other fields to ensure all factors are considered.

Ultimately, we believe that, if made easy and affordable, users can be encouraged to consider security and sustainability in their IoT purchasing decisions. Security is not the least important motivation to retire an IoT device and with some effort by designers and vendors, this consideration can be increased. Encouraging, and eventually requiring modularity in IoT devices will help users buy into better IoT security hygiene, and help the planet along the way.

Acknowledgments

We would like to thank our shepherds, Dr. Ingolf Becker and Dr. Scott Ruoti, for their guidance and support in revising this paper. We would also like to thank the NSPW 2024 attendees for their questions, comments and discussion about our work which have contributed to the final version of this paper.

This work was financially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC). Keleher was supported through a PGS-D scholarship, and Barrera and Chiasson through Discovery Grants.

References

[1] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. 2019. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 451–466. https://www.usenix.org/conference/soups2019/presentation/abdi

[2] Wael S Albayaydh and Ivan Flechais. 2022. Exploring Bystanders' Privacy Concerns with Smart Homes in Jordan. In *CHI Conference on Human Factors in Computing Systems*. ACM, New Orleans LA USA, 1–24. https://doi.org/10.1145/3491102.3502097

[3] Manos Antonakakis, Tim April, Michael Bailey, Matthew Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou. 2017. Understanding the mirai botnet. In *Proceedings of the 26th USENIX Conference on Security Symposium* (Vancouver, BC, Canada) *(SEC'17)*. USENIX Association, USA, 1093–1110.

[4] Hany F. Atlam and Gary B. Wills. 2020. IoT Security, Privacy, Safety and Ethics. In *Digital Twin Technologies and Smart Cities*, Maryam Farsi, Alireza Daneshkhah, Amin Hosseinian-Far, and Hamid Jahankhani (Eds.). Springer International Publishing, Cham, 123–149. https://doi.org/10.1007/978-3-030-18732-3_8 Series Title: Internet of Things.

[5] Gabriela Baron. 2023. Design for Conservation (D4C): A Toolkit That Enables Sustainable, Collaborative, and Distributed Innovation. In *Design for Adaptation Cumulus Conference Proceedings Detroit 2022*. Cumulus, USA, 749–764. https://www.research.ed.ac.uk/en/publications/towards-sustainable-internet-of-things-objects-design-strategies-

[6] Gabriela Nuri Barón and Nadereh Ghelich Khani. 2021. Defining Design for Sustainability and Conservation Mindsets. *Cuadernos del Centro de Estudios de Diseño y Comunicación* 132 (June 2021), 131–151. https://doi.org/10.18682/cdc.vi132.4983

[7] Antonio G. Di Benedetto. 2024. *Spotify is refunding Car Thing owners before bricking their devices*. The Verge. https://www.theverge.com/2024/5/30/24168081/spotify-car-thing-end-of-life-customer-refund

[8] Elisa Bertino. 2019. IoT Security A Comprehensive Life Cycle Framework. In *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*. IEEE, Los Angeles, CA, USA, 196–203. https://doi.org/10.1109/CIC48465.2019.00033

[9] Conner Bradley and David Barrera. 2023. Escaping Vendor Mortality: A New Paradigm for Extending IoT Device Longevity. In *New Security Paradigms Workshop*. ACM, Segovia Spain, 1–16. https://doi.org/10.1145/3633500.3633501

[10] B. N. Bridgens, D. Lilley, G. Smalley, and K. Balasundaram. 2015. Ageing gracefully to increase product longevity. In *PLATE: Product Lifetimes and The Environment*. Newcastle University, Newcastle, England, 19–26.

[11] Cameron Camp and Anscombe, Tony. April 2023. *How I (could've) stolen your corporate secrets for $100.* White Paper. ESET Research.

[12] Ann Cavoukian. 2010. Privacy by design: The 7 foundational principles. , 5 pages. Publisher: Office of the Information and Privacy Commissioner.

[13] Jason Ceci, Hassan Khan, Urs Hengartner, and Daniel Vogel. 2021. Concerned but Ineffective: User Perceptions, Methods, and Challenges when Sanitizing Old Devices for Disposal. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, USA, 455–474. https://www.usenix.org/conference/soups2021/presentation/ceci

[14] Tim Cooper. 2004. Inadequate Life? Evidence of Consumer Attitudes to Product Obsolescence. *Journal of Consumer Policy* 27, 4 (Dec. 2004), 421–449. https://doi.org/10.1007/s10603-004-2284-6

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

[16] Federal Communications Commission. 2013. CHILDREN'S ONLINE PRIVACY PROTECTION RULE. https://www.ecfr.gov/current/title-16/part-312

[17] Federal Communications Commission. 2024. FCC Adopts Rules for IoT Cybersecurity Labeling Program. https://www.fcc.gov/document/fcc-adopts-rules-iot-cybersecurity-labeling-program

[18] Kiri Feldman and Peter Sandborn. 2007. Integrating Technology Obsolescence Considerations Into Product Design Planning. In *Volume 4: ASME/IEEE International Conference on Mechatronic and Embedded Systems and Applications and the 19th Reliability, Stress Analysis, and Failure Prevention Conference*. ASMEDC, Las Vegas, Nevada, USA, 981–988. https://doi.org/10.1115/DETC2007-35881

[19] Nathaniel Fruchter and Ilaria Liccardi. 2018. Consumer Attitudes Towards Privacy and Security in Home Assistants. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, Montreal QC Canada, 1–6. https://doi.org/10.1145/3170427.3188448

[20] O. Garcia-Morchon, S. Kumar, and M. Sethi. 2019. *Internet of Things (IoT) Security: State of the Art and Challenges.* Technical Report RFC8576. RFC Editor. RFC8576 pages. https://doi.org/10.17487/RFC8576

[21] Simson L Garfinkel and Abhi Shelat. 2003. Remembrance of data passed: A study of disk sanitization practices. *IEEE Security & Privacy* 1, 1 (2003), 17–27.

[22] Craig Goodwin and Sandra Woolley. 2024. Barriers to device longevity and reuse: A vintage device empirical study. *Journal of Systems and Software* 211 (May 2024), 111991. https://doi.org/10.1016/j.jss.2024.111991

[23] Komal Habib, Elham Mohammadi, and Sohani Vihanga Withanage. 2023. A first comprehensive estimate of electronic waste in Canada. *Journal of Hazardous Materials* 448 (April 2023), 130865. https://doi.org/10.1016/j.jhazmat.2023.130865

[24] Julie M. Haney, Susanne M. Furman, and Yasemin Acar. 2020. Smart Home Security and Privacy Mitigations: Consumer Perceptions, Practices, and Challenges. In *HCI for Cybersecurity, Privacy and Trust*, Abbas Moallem (Ed.). Vol. 12210. Springer International Publishing, Cham, 393–411. https://doi.org/10.1007/978-3-030-50309-3_26 Series Title: Lecture Notes in Computer Science.

[25] Laura Hennies and Rainer Stamminger. 2016. An empirical survey on the obsolescence of appliances in German households. *Resources, Conservation and Recycling* 112 (Sept. 2016), 73–82. https://doi.org/10.1016/j.resconrec.2016.04.013

[26] Stacey Higginbotham. 2018. The Internet of Trash: IoT Has a Looming E-Waste Problem - IEEE Spectrum. https://spectrum.ieee.org/the-internet-of-trash-iot-has-a-looming-ewaste-problem

[27] Stacey Higginbotham. 2020. The IoT's E-Waste Problem Isn't Inevitable - IEEE Spectrum. https://spectrum.ieee.org/the-iots-ewaste-problem-isnt-inevitable

[28] Toshiaki Iizuka. 2007. An Empirical Analysis of Planned Obsolescence. *Journal of Economics & Management Strategy* 16, 1 (March 2007), 191–226. https://doi.org/10.1111/j.1530-9134.2007.00137.x

[29] Melanie Jaeger-Erben, Vivian Frick, and Tamina Hipp. 2021. Why do users (not) repair their devices? A study of the predictors of repair practices. *Journal of Cleaner Production* 286 (March 2021), 125382. https://doi.org/10.1016/j.jclepro.2020.125382

[30] Andrew Jones, Olga Angelopoulou, and Len Noriega. 2019. Survey of data remaining on second hand memory cards in the UK. *Computers & Security* 84 (2019), 239–243.

[31] Adam Khalid, Usha Sakthivel, Senthilkumaran Thangamuthu, Micheal Drieberg, Patrick Sebastian, Azrina Abd Aziz, and Lo Hai Hiung. 2022. Extended Lifetime of IoT Applications using Energy Saving Schemes. In *2022 International Conference on Future Trends in Smart Communities (ICFTSC)*. IEEE, Kuching, Sarawak, Malaysia, 93–97. https://doi.org/10.1109/ICFTSC57269.2022.10040064

[32] Daniel A. Levinthal and Devavrat Purohit. 1989. Durable Goods and Product Obsolescence. *Marketing Science* 8, 1 (Feb. 1989), 35–56. https://doi.org/10.1287/mksc.8.1.35

[33] Yuting Liao, Jessica Vitak, Priya Kumar, Michael Zimmer, and Katherine Kritikos. 2019. Understanding the Role of Privacy and Trust in Intelligent Personal Assistant Adoption. In *Information in Contemporary Society*, Natalie Greene Taylor, Caitlin Christian-Lamb, Michelle H. Martin, and Bonnie Nardi (Eds.). Vol. 11420. Springer International Publishing, Cham, 102–113. https://doi.org/10.1007/978-3-030-15742-5_9 Series Title: Lecture Notes in Computer Science.

[34] Christoph Lutz and Gemma Newlands. 2021. Privacy and smart speakers: A multi-dimensional approach. *The Information Society* 37, 3 (May 2021), 147–162. https://doi.org/10.1080/01972243.2021.1897914

[35] Batoul Modarress Fathi, Alexander Ansari, and Al Ansari. 2022. Threats of Internet-of-Thing on Environmental Sustainability by E-Waste. *Sustainability* 14, 16 (Aug. 2022), 10161. https://doi.org/10.3390/su141610161

[36] Mariale Moreno, Carolina De Los Rios, Zoe Rowe, and Fiona Charnley. 2016. A Conceptual Framework for Circular Design. *Sustainability* 8, 9 (Sept. 2016), 937. https://doi.org/10.3390/su8090937

[37] Kavous Salehzadeh Niksirat, Diana Korka, Quentin Jacquemin, Céline Vanini, Mathias Humbert, Mauro Cherubini, Sylvain Métille, and Kévin Huguenin. 2024. Security and Privacy with Second-Hand Storage Devices: A User-Centric Perspective from Switzerland. *Proceedings on Privacy Enhancing Technologies (PoPETs)* 2024, 2 (2024), 22.

[38] Matthew Pilling, Michael Stead, Adrian Gradinar, Christian Remy, and Thomas Macpherson-Pope. 2023. Preparing to Repair: Using Co-Design and Speculative Design Methods to Explore the Future of IoT Right-to-Repair with Citizens and Communities. In *Design for Adaptation Cumulus Conference Proceedings Detroit 2022*. Cumulus, USA, 482–501. https://www.research.ed.ac.uk/en/publications/towards-sustainable-internet-of-things-objects-design-strategies-

[39] Leila Fatmasari Rahman, Tanir Ozcelebi, and Johan Lukkien. 2018. Understanding IoT Systems: A Life Cycle Approach. *Procedia Computer Science* 130 (2018), 1057–1062. https://doi.org/10.1016/j.procs.2018.04.148

[40] Rahul Rai and Janis Terpenny. 2008. Principles for Managing Technological Product Obsolescence. *IEEE Transactions on Components and Packaging Technologies* 31, 4 (Dec. 2008), 880–889. https://doi.org/10.1109/TCAPT.2008.2005115

[41] Joel Reardon, David Basin, and Srdjan Capkun. 2013. SoK: Secure Data Deletion. In *2013 IEEE Symposium on Security and Privacy*. IEEE, USA, 301–315. https://doi.org/10.1109/SP.2013.28

[42] Julio L. Rivera and Amrine Lallmahomed. 2016. Environmental implications of planned obsolescence and product lifetime: a literature review. *International Journal of Sustainable Engineering* 9, 2 (March 2016), 119–129. https://doi.org/10.1080/19397038.2015.1099757

[43] Mostafa Sabbaghi, Behzad Esmaeilian, Willie Cade, Kyle Wiens, and Sara Behdad. 2016. Business outcomes of product repairability: A survey-based study of consumer repair experiences. *Resources, Conservation and Recycling* 109 (May 2016), 114–122. https://doi.org/10.1016/j.resconrec.2016.02.014

[44] Burkhard Schafer. 2014. D-waste: data disposal as challenge for waste management in the Internet of Things. *The International Review of Information Ethics* 22 (2014), 101–107.

[45] Scharon Harding. 2024. *Amazon Will Brick Its $2,350 Astro Robots Just 10 Months After Release*. Wired. https://arstechnica.com/gadgets/2024/07/amazon-is-bricking-2350-astro-robots-10-months-after-release/ Section: tags.

[46] Tianfeng Shi, Rong Huang, and Emine Sarigöllü. 2022. Consumer product use behavior throughout the product lifespan: A literature review and research agenda. *Journal of Environmental Management* 302 (Jan. 2022), 114114. https://doi.org/10.1016/j.jenvman.2021.114114

[47] Pameet Singh and Peter Sandborn. 2006. Obsolescence Driven Design Refresh Planning for Sustainment-Dominated Systems. *The Engineering Economist* 51, 2 (July 2006), 115–139. https://doi.org/10.1080/00137910600695643

[48] Michael Stead, Paul Coulton, Joseph Lindley, and Claire Coulton. 2019. *The Little Book of SUSTAINABILITY for the Internet of Things*. Lancaster University, Lancaster, England.

[49] Iain Sutherland, Gareth Davies, Andy Jones, and Andrew J. C. Blyth. 2010. Zombie Hard disks - Data from the Living Dead. *8th Australian Digital Forensics Conference* Edith Cowan University (2010), 156–161. https://doi.org/10.4225/75/

57B2B48D40CE3
[50] James Thorp, Susan Lechelt, Luis Soares, Katerina Gorkovenko, Chris Speed, Michael Stead, Nick Dunn, and Daniel Richards. 2023. Towards Sustainable Internet of Things Objects Design Strategies for End-of-Life. In *Design for Adaptation Cumulus Conference Proceedings Detroit 2022*. Cumulus, USA, 622–639. https://www.research.ed.ac.uk/en/publications/towards-sustainable-internet-of-things-objects-design-strategies-
[51] UK Parliament. 2022. Product Security and Telecommunications Infrastructure Act 2022. https://www.legislation.gov.uk/ukpga/2022/46/contents
[52] Rūta Valušytė. 2023. Design for circular business models: a conceptual framework. In *Design for Adaptation Cumulus Conference Proceedings Detroit 2022*. Cumulus, USA, 734–748. https://www.research.ed.ac.uk/en/publications/towards-sustainable-internet-of-things-objects-design-strategies-
[53] Renske van den Berge, Lise Magnier, and Ruth Mugge. 2021. Too good to go? Consumers' replacement behaviour and potential strategies for stimulating product retention. *Current Opinion in Psychology* 39 (June 2021), 66–71. https://doi.org/10.1016/j.copsyc.2020.07.014
[54] W. Kip Viscusi, Joel Huber, and Jason Bell. 2012. Alternative Policies to Increase Recycling of Plastic Water Bottles in the United States. *Review of Environmental Economics and Policy* 6, 2 (July 2012), 190–211. https://doi.org/10.1093/reep/res006
[55] Artem Voronkov, Leonardo Horn Iwaya, Leonardo A. Martucci, and Stefan Lindskog. 2017. Systematic Literature Review on Usability of Firewall Configuration. *ACM Comput. Surv.* 50, 6, Article 87 (dec 2017), 35 pages. https://doi.org/10.1145/3130876
[56] Maximiliane Windl and Sven Mayer. 2022. The Skewed Privacy Concerns of Bystanders in Smart Environments. *Proceedings of the ACM on Human-Computer Interaction* 6, MHCI (Sept. 2022), 1–21. https://doi.org/10.1145/3546719
[57] Peter Zdankin and Torben Weis. 2020. Longevity of Smart Homes. In *2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. IEEE, Austin, TX, USA, 1–2. https://doi.org/10.1109/PerComWorkshops48775.2020.9156155
[58] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security & privacy concerns with smart homes. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security* (Santa Clara, CA, USA) *(SOUPS '17)*. USENIX Association, USA, 65–80.
[59] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (Nov. 2018), 1–20. https://doi.org/10.1145/3274469

A Questionnaire

Types of Devices

See Table 2

Device Specific Questions

(1) How long do you expect a [IoT/Non-IoT device] to last (from time of purchase)?
(2) How long do you expect the manufacturer to offer parts to repair [IoT/Non-IoT device]?
(3) How long do you expect the manufacturer to offer software updates for [IoT device]?
(4) How long do you expect the manufacturer to offer security updates for [IoT device]?
(5) How long have you owned your current [IoT device]?

Device Retirement Questions

(1) Please rank the importance of the following reasons to stop using an IoT device:
   - The device no longer worked
   - I wanted to have a new model
   - I found a model with a more attractive design
   - A new device gives me joy
   - I felt that I had used my last device long enough
   - Because I found a special offer for a new device
   - Because I felt the device was insecure
   - Because I felt that device was collecting personal information

(2) If you replaced or discarded an IoT device for a reason not listed, please describe it here and indicate its importance relative to the other reasons listed above. (Optional) [Textbox]
(3) Please describe what you did with the last IoT device you stopped using? [Textbox]

General IoT Questions

(1) It is important for me to use IoT devices with the latest technology or features. [strongly agree, agree, neutral, disagree, strongly disagree]
(2) It is a great feeling to own a brand new IoT device. [strongly agree, agree, neutral, disagree, strongly disagree]
(3) Which IoT devices are more secure? [Older IoT devices are much more, older IoT devices are somewhat more, they are equally, newer IoT devices are somewhat more, newer IoT devices are much more]
(4) Which IoT devices are more privacy preserving? [Older IoT devices are much more, older IoT devices are somewhat more privacy preserving, they are equally, newer IoT devices are somewhat more, newer IoT devices are much more]
(5) Which devices are more secure? [IoT devices are much more secure, IoT devices are somewhat more, they are equally, non-IoT devices are somewhat more, non-IoT devices are much more]
(6) Which devices are more privacy preserving? [IoT devices are much more, IoT devices are somewhat more, they are equally, non-IoT devices are somewhat more, non-IoT devices are much more]

Demographic Questions

(1) Which of the following best describes your gender identity? [Woman, Non-binary, Man, Not listed (Please specify), Prefer not to say]
(2) How old are you (in years)? [Numeric entry]
(3) Which country do you currently live in? [Canada, United States of America]
(4) Do you have experience in computer science, information technology, computer/software engineering, or a related field? [Yes (please describe), No]

Concluding Questions

(1) Is there anything else you would like to share about IoT device longevity and disposal (Optional)?
(2) Do you have any feedback you would like to share about the survey (Optional)?

B Additional descriptive statistics

Table 7: Mean number of years for that participants (i) owned their devices, (ii) expected them to last, (iii) expected them to have parts available for repair, and (iv) expected that they would receive software updates. 'Non' = Non-IoT devices.

Category	Owned	Lifespan		Repair		Updates	
	IoT	IoT	Non	IoT	Non	Functional	Security
TV	5.0	8.1	12.2	7.2	8.6	6.5	7.5
Monitoring	3.0	6.4	8.6	5.5	5.8	5.2	6.2
Emergency alerts	3.6	8.9	11.4	7.2	8.3	7.2	7.6
Large appliances	3.7	11.4	14.7	9.8	11.4	8.6	9.0
Small appliances	2.7	7.0	9.2	6.1	6.6	5.5	5.8
Lights	4.2	5.4	3.9	4.4	4.0	4.3	4.5
Home automation	4.3	9.6	12.5	7.6	8.8	7.3	7.5