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

Tanvi Vats, TV, Vats[*]

School of Computer Science, University of Nottingham, tanvi.vats@nottingham.ac.uk

Neelima Sailaja, NS, Sailaja

Horizon Digital Economy Hub, School of Computer Science, University of Nottingham, neelima.sailaja@nottingham.ac.uk

Fabiana Anselmo Polido Lopes, FAPL, Anselmo

Mixed Reality Laboratory, School of Computer Science, University of Nottingham, fabiana.anselmo@nottingham.ac.uk

As the uptake of Internet of Things (IoT) exacerbates, questions around the environmental impacts of its making and maintenance call to be considered with urgency. Here, the inherent unsustainable nature of these devices has rarely been considered., e.g., shorter lifespans, large amounts of data collected, and the obsolescence caused by the software that runs them. This study highlights such instances of pre-mature software obsolescence of domestic IoT devices and understands user expectations on how to tackle them. We used 5 textual scenarios to drive 8 focus group sessions with 34 participants. Findings reveal user perceptions of the role of different IoT repair actors in tackling existing software challenges and the importance of repair for reusing them. Our contribution highlights three key sets of stakeholder (users, manufacturers, and regulators) focused recommendations for IoT design that embodies repairability, while contextualising and highlighting HCI's key role in this emergent space.

CCS CONCEPTS • Human-centered computing • Human computer interaction (HCI) • Empirical studies in HCI

Additional Keywords and Phrases: Internet of Things (IoT), Repair, Software, Sustainability

This submission was supported by the EPSRC Grant Number EPSRC EP/W024780/1 and ESRC ES/X502352/1. Any enquiries regarding this submission should be sent to horizon@nottingham.ac.uk.

[*] Corresponding author.

ACM Reference Format:

First Author's Name, Initials, and Last Name, Second Author's Name, Initials, and Last Name, and Third Author's Name, Initials, and Last Name. 2018. The Title of the Paper: ACM Conference Proceedings Manuscript Submission Template: This is the subtitle of the paper, this document both explains and embodies the submission format for authors using Word. In Woodstock '18: ACM Symposium on Neural Gaze Detection, June 03–05, 2018, Woodstock, NY. ACM, New York, NY, USA, 10 pages. NOTE: This block will be automatically generated when manuscripts are processed after acceptance.

1 Introduction

E-waste is the fastest growing waste stream globally and it has been increasing at the rate of 3-5% annually in Europe. [90, 105] It degrades the environment by increasing greenhouse gas emissions through excessive production, and depletion of the world's physical resources. From a social perspective, it contributes to a stark digital device with many developed countries in the West, exporting their e-waste to developing countries like India, Bangladesh, and Congo, affecting entire villages, especially young children and women who primarily engage in such waste processing. [46, 97] The exponential growth of internet of connected devices [49, 70], including Internet of Things (IoT) embedded products, has exacerbated this problem further. Current responses to this global concern originate from different levels of society, starting from legal responses like the Right to Repair [102] or France's repairability scores [52] on goods to economic theories around and methodologies of the Circular Economy [106] to academic discourses [35, 41] to most recently the rise of repair cafes: independent international grassroots movement happening all over the world. [107–111]

Research has highlighted the importance of making human-repair interactions meaningful, usable, and culturally aware to incentivise repair activities envisioned under the R2R movement. [2, 38, 63] However, these studies have primarily addressed hardware obsolescence in EEE and ICT products so far. Within HCI, focus around IoT has recently been on implications on user privacy and security and how to mitigate those risks. [11, 12, 15, 89] HCI researchers have recognised this gap and in recent years various approaches are being taken to examine the scope of repairability in IoT design. [73–77] However, the effects of technology, software and data-related challenges, their manifestations on IoT lifecycle and its (dis)use by users have not been considered so far.

This study aims to explore and contextualise instances of IoT design and personal use within domestic contexts where technological, software and data-related concerns exist at various points in its lifecycle and gather user feedback on their expectations around response and repair in these scenarios. We designed 5 textual scenarios to represent diverse instances of software and data faults around IoT domestic contexts and used them as probes to drive focus groups with users. Our results explicate user perceptions of the role of key repair actors (users, manufacturers, and regulators) in upholding the maintainability and repairability of IoT devices, IoT specific software related challenges and concerns around the reuse of repaired devices. Our contribution here is twofold. First, we conclude by identifying three sets of *stakeholder focused recommendations for IoT design that embodies repairability*. These are IoT related *user challenges* (that include data interactions, internet independence, privacy, and security) which call for a *revision in the role of the manufacturers* and a need for better support from *regulatory authorities.* Second, we simultaneously contextualise the recommendations within multidisciplinary literature while drawing out the scope for HCI intervention here hence, highlighting to the HCI community its position as a key player within this emergent area.

2 LITERATURE REVIEW

IoT is a network of 'things' – anything and everything that can be connected to the internet. [76] In 2020, for the first time, there were more IoT connections (e.g., smart home devices and connected cars) than non-IoT connections (e.g., smartphones, laptops, and computers) globally. [49] Their use has posed serious concerns around security [112], privacy [58], and environmental sustainability. [45] While sustainability studies in IoT have focused on using them to promote sustainable behaviours [4, 8, 22, 27, 87], they have overlooked the unsustainable nature of the 'things' themselves. Despite their benefits, IoT devices are still being designed, manufactured, and disposed irresponsibly, much like majority of the consumer goods have been for decades in the current linear economy. [76]

2.1 Circular Economy and Repair – Barriers and Opportunities

Circular Economy is based on three design-driven principles: 1) eliminating waste and pollution 2) circulating products and materials at their highest value and, 3) regenerating nature. Reuse and repair form the innermost loops in various CE models. [113] These processes retain the highest value of the products being used and are integral to stopping waste from entering the landfills. [114]

Consumer products in the market have been seeing a trend of declining durability and repairability. [90, 115] Things break. Manufacturers have been designing products for 'limited repair' using tactics such as limiting the supply of replacement components, thereby making it impossible to repair or modify products when needed. [37, 65] Similarly, discontinuing after-sales maintenance support, including software support, have also forced users to replace products that are still operational. For example, Microsoft's decision to discontinue Windows 10 OS could push over 240 million personal computers straight to landfills. [72] In the past, companies like Apple and Samsung too have been accused of using software updates to slow down their phones. [29]

Product designs can intentionally or inadvertently hinder repair. Designing complex circuitry and sealing subcomponents using tamper-resistant mechanisms have also limited the repairability of electronic products. [18] Moreover, by using monopolistic practices such as serialisation and part-pairing, the tech industry has been accused of preventing and disincentivising third-party repairs. [50] Independent repairers also find it hard to gain users' trust and confidence due to data privacy concerns and a fear of being exploited. [10, 65] These effects are exacerbated for the everyday user due to their unwavering trust in manufacturer services [61], lack of basic repair and technical skills and unavailability of accessible and timely repair information. [48]

Making repairs harder has socio-economic ramifications too. Short product lifetimes adversely affect low-income groups. They are less likely to take risks with buying high-value products because of a perception of rampant planned obsolescence in electronics design, ending up with cheaper, low-value products which can be easily replaced. [69] They focus on meeting their more immediate needs and therefore products which fail or break outside the warranty period are most likely to be discarded than repaired. [51] Alternatively, affluent households typically dispose products rather than repair them due to business practices that incentivise replacement over repair (such as trade-in policies). [69]

There are also vast imbalances in credit and compensation accorded to repair compared to production of new technologies. [38] This in turn has led to a negative perception around technological products that have been repaired. However, in recent years, several repair communities and maker spaces have propped up across the globe and researchers have meditated on values of collaboration, learning and community building embedded in repair. [62, 63] These sites have been built on principles of user empowerment, knowledge-sharing and environmental responsibility and have been successful in engaging communities to reflect on their relationships with material objects. [62, 77] Despite their noble principles, DIY repair cultures are specialist spaces and often gender coded with tech-repair largely undertaken by men, as women either lack confidence or motivation to repair and/or are perceived to be less competent to participate. [2, 62, 63]

2.2 'Right to Repair' Movement

Non-Governmental Organisations (NGOs) like The Restart Project [109] and iFixit [103] offer tools, repair guides and resources, and their advocacy for repair have played a pivotal role in promoting repair-friendly practices. Their demands for a legal 'Right to Repair' have gained momentum in different parts of the world for the right to freely modify and repair products without any manufacturer-imposed barriers. [102] Multiple states in the US such as California and New York [116] and economic regions like the European Union (EU) [94], United Kingdom

(UK) [17], Australia [92], and India [117] have passed their versions of repair laws and eco-directives. These laws give users the right to disassemble their products, easily source parts and tools needed for repair, and get them fixed *anywhere*. EU's Eco-design Working Plan [118] and the Waste Electrical and Electronic Equipment (WEEE) Directive [119], also encourages manufacturers to design products with repairability, reuse, and recycling in mind.

Corporate efforts to promote repair-friendly design have been crucial with companies like Fairphone [120], Framework [121] and Nokia [122] adopting modularity and eco-design principles to make products easier to disassemble and repair. New business models like product-service systems are also aligning with environmental and social concerns. [60]

Additionally, countries like Sweden offer tax breaks for repair and reduced VAT on repairable products, while Austria, France, Germany, US, and the Nordic countries use eco-signalling practices such as labels, standards, and certifications to distinguish durable and repair-friendly products in the market. [71] Currently, none of these efforts directly address repair challenges associated with IoT products.

2.3 IoT Repair

In [73–76], researchers designed a series of design fiction prototypes to conceptualise sustainable and responsible IoT design practices. Using a research-through-design approach, they unveil tensions between current unsustainable practices and these fictitious circular alternatives, re-envisioning business models and user behaviours, policy and innovation, and ethics and ownership, and present readers with a world where modular, customisable, upgradable, repairable, and recyclable smart toasters exist within a legal space that promotes open-source hardware, crowdfunding, and regulated DIY IoT innovation where products carry their meta-histories with themselves even if moving from one person to another. Though radical, this auto-research has not been informed by user input and does not consider their interactions and perceptions.

A series of workshops with local communities, including end-users, found that participants overwhelmingly distrusted IoT manufacturers' ongoing unsustainable practices (such as not supporting the software and/or associated service platforms even if the devices' hardware remains functional) and were increasingly adopting professionally refurbished products these past few years. [77] The finding offers a different perspective from enthusiast communities, when compared to those observed in repair studies with general users, discussed in section 2.1. where they preferred replacing their devices with newer ones. However, despite the discussions around software obsolescence, this workshop too focused on introducing diagnostic and repair toolkits for encouraging hardware tinkering in an enthusiast community.

2.4 Missing Focus on Software

In [68], software repair was seen as the practice of updating older smartphones, which were no longer supported by the manufacturers, to their latest versions. Some researchers have developed a series of conceptual plug-ins to help users protect themselves and customise smartphone applications that better suit their needs [43]. Others have studied how users interact with simple algorithms for smart spaces [88] and have underscored the need to create interfaces that proactively support effective end-user debugging for affording them with greater software control [7]. The open-source software movement also lends support to the demands for a right to repair software but is challenged by various laws around intellectual property and copyright laws. [6] The writer in [31] however argues that the most important issues related to software repair do not involve user's ability to fix the bugs themselves, but their ability to manage (demanding or refusing) the updates from software developers and to revert to an older version of the software to continue to use the device.

In a 2019 report by the UK Government Environmental Audit Committee [90], less than 1% of repair organisations saw software as a barrier to repair. However, recent instances related to consumer IoT devices have highlighted egregious instances of software-induced obsolescence.

For example, large quantities of Chromebooks that were procured by public schools in the US to enable remote learning during COVID-19 are facing the threat of software support cut off by the manufacturers just three years after purchase, that could result in a huge pile of e-waste and a massive economic cost of 1.8 billion USD. [16] In another peculiar event, a district school in Massachusetts had 7000 of its smart lights turned on for over a year due to a software snag that couldn't be fixed because the installer lost the propriety software embedded on the system. [96] A recent UK report has also revealed that an estimated 7 million smart meters are at a risk of being bricked by losing data connectivity by 2033. [123] These instances reveal technological and software related issues that manifest at different points in the lifecycle of an IoT device that fall beyond the conventional discussions around repair.

In addition to these, IoT devices also collect large amounts of user data for their day-to-day functioning and has attracted research around privacy and cybersecurity concerns associated with them. [11, 12, 15, 89] Questions around data legibility and portability have also been considered. [66] However, effects of such data-related interactions associated with repair haven't been considered. In [30], of the 86 second-hand Amazon Echo Dots researchers purchased from re-sellers, 61% of them had not been reset by previous owners. Examples such as that of Google Nest cameras which allowed previous owners to peer into the homes of its new owners also raise critical questions around existing reset mechanisms. [58]

The intangibility and ubiquity of software and data-related interactions relegate them into the background, making their effects on the lifecycle of the IoT largely invisible in the current discourse around repair and maintenance. Therefore, there is a need to make visible these invisible effects on the lifecycle of IoT and understand expectations on how to repair and reverse such pre-mature obsolescence by talking to the first responders – the users.

3 Methodology

A combination of scenario-based exploration, focus group discussions and written responses were used to gather information to explore user attitudes and preferences towards handling of software and data related issues related to IoT devices.

Scenarios are a set of narratives that describe what people do in a particular context. [101] When used in an interview, scenarios can help focus the participant on a particular situation to elicit reflection and responses within that context. [5, 26, 59] In this study, textual scenarios were used as provocations to highlight shortcomings in software and data-related interactions in current IoT design and encourage new, critical thinking from participants. [124] Our goal in writing them was to open, rather than conclude, discussions and to promote critical engagement with the status quo. [9] Since the aim of the study was to gauge participant attitudes and preferences to build an understanding of their interactions with the technology, focus groups were used as the primary method of data collection.

Focus groups offer the benefits of semi-structured interviews by allowing for clarifications and help in gathering a broad range of viewpoints and insights, at the same time. [42, 57] However, as focus groups can sometimes be held hostage to poor group dynamics or social interactions, participants in our study were allowed to submit written responses instead of verbal responses too. Written responses also offered us the benefit of capturing a participants' original insights and mitigating group effect. [54]

A pre-questionnaire was used to collect participant demographic information (age, gender, occupation, and location) and gather information about the kinds, general attitudes, perceived benefits, and concerns associated with smart devices. This information, along with their availability, was used to make groups for the user sessions.

3.1 Definitions

We define what we refer as an 'IoT device' and 'manufacturer' in our study.

3.1.1IoT Device

Internet of Things (IoT) is a network of physical devices (including vehicles, appliances, and other physical objects) that are embedded with software, sensors and network connectivity that allows them to collect and share data. [100] Whereas, smart devices are everyday objects made intelligent with advanced computing, which can be networked to form the internet of things (IoT). They can be a subset of IoT. [125] Connected devices are connected to the internet to exchange information. [100] Our study considers an IoT device as an umbrella of these terms. We have considered end-point devices which can collect and transmit data over the internet and can provide internet-enabled smart functionality. This is because most users focus on just one or two smart home devices/functions instead of full home automation. [126] Therefore, we have not studied network effects between different devices in our study. Additionally, we have limited our study to consumer personal IoT devices. We collectively refer to them as an 'IoT device' in this paper.

3.1.2Manufacturer

There are multiple stakeholders involved in the production and maintenance of an IoT device such as the device manufacturers, IoT service providers, mobile application developers and retailers. [127] However, for the sake of simplicity in a user focused study we have clubbed non-user stakeholders together as 'manufacturer' in this paper.

3.2 Scenario Design

The textual scenarios were designed in three stages. In the first stage, desk research was conducted to collect past and current examples of software and data-related instances associated with the use and post-use phases of household IoT devices (such as washing machines [45, 99], connected cars [93, 128], smart lighting [96, 129] smart speakers [30] and cameras [58]) that had led or could lead to their obsolescence. In the second stage, triggers to obsolescence were identified in each example. Similar examples were grouped under a common theme. Five technological, software and data-related themes for the scenarios were derived, namely, 1) malicious updates and cyberattacks 2) limited software support 3) changes in supporting infrastructure 4) software ownership and 5) resetting problems in second-hand IoT. In the third stage, examples under each theme were synthesised to develop a textual scenario to provoke discussions with the participants. For complete text of these scenarios, see Appendix A.1.

3.3 Participants

Participants were recruited through a combination of purposive sampling, convenience sampling and snowball sampling [47, 78] and was open to persons with all levels of technical experience, above the age of 18 and based in the United Kingdom with at least one IoT device at home. The recruitment drive used communication channels including poster advertisements across the University of Nottingham campus, department-wide e-mails, social media networking sites such as LinkedIn and WhatsApp and personal messaging.

The study had 34 participants (13 female and 21 male) with an age range of 18 to 67 years, from varying educational and occupational backgrounds such as students (from computer science, human-computer interaction, graphic design, and microbiology), graphic designers, law professionals, project managers, software engineers and homemakers. All participants were based in the UK and joined the study from Nottingham, Bournemouth, London, Manchester, York, Lancashire, Bristol, Birmingham, and Cheshire and were familiar with IoT devices at home. Since the sample was made up of diverse groups of people, allowing us to gather a variety of perspectives on the research topic, the study upholds good generalizability.

3.4 User Sessions

All focus group discussions were conducted over MS Teams. Each session was 2 hours long and a total of 8 focus group sessions were conducted with participants ranging between 2 to 7 in each group. Most sessions consisted of

3 participants (mode). (2-1, 3-3, 4-2, 5-1, 7-1) A second researcher acted as a moderator during data collection to reduce researcher bias and introduce reflexivity in the study design. [44]

The 5 scenarios were sent to the participants as MS Word files, with instructions on how to download them and join the Teams meeting, 30 minutes before the user sessions. We used MS Word due to its familiarity and in-built accessibility features allowing our diverse group of participants to easily access the contents of the scenarios. During the sessions, researchers and participants introduced themselves and participants were encouraged to turn their cameras on, however this was optional. Each scenario presentation included 5-7 minutes of individual reading of the textual scenario and participants were encouraged to make notes on the file, followed by a 15-minute group discussion. Participants were also offered a 5–10-minute break after three scenarios. They were compensated with a 10 GBP Amazon voucher for their time and effort after the user sessions were completed.

The ethics for the study was approved by the School's Ethics Review Committee. All participants were served an information sheet and consent form online to be completed before participation in the sessions. The raw data was prepared by transcribing and anonymising the recorded audio files of the user sessions and written responses in line with GDPR regulations. The analysis was conducted using thematic analysis methods [7], driven by grounded theory philosophy [77], which involved an iterative cycle of data familiarisation by manually transcribing audio data and adding observational and analytical notes, creation of codes that emerged naturally from the data, searching for themes and sub-themes by combining similar codes, reviewing the themes for semantic and conceptual flow, naming and defining these themes and writing up the themes by bringing together the analytic narrative, data extracts and the wider HCI discourse on the subject.

3.5 Limitations and Scope

This study includes participation from individuals with basic familiarity with IoT devices and does not consider the IoT repair and maintenance needs of persons who are currently not familiar with IoT technology or have used IoT devices, therefore exhibiting a different learning curve. Additionally, the scenarios focus on personal use of the IoT devices and do not consider effects of device sharing, which can influence repair and maintenance behaviour due to distributed ownership and shared data-management practices. [86] Moreover, the study is geographically limited to the UK and does not reflect user experiences in different cultural contexts which can also shape how users interpret and interact with instances of obsolescence, repair, and maintenance. [38]

4 Findings

In navigating IoT repair, users seek fair partnerships with manufacturers, balancing ownership of hardware with reliance on software support. They advocate for clearer communication and industry standards to address concerns about complex user agreements and lack of control. Participants emphasize the importance of trust in manufacturers for resolving software issues and negotiate for extended support periods. Additionally, they express hesitancy in purchasing second-hand devices without manufacturer support and call for better design for reusability.

4.1 User, Manufacturer and Regulator: The Current Triad of IoT Repair

Users see ownership as shared between themselves and manufacturers, with control over hardware but reliance on manufacturers for software updates due to lack of expertise and security concerns. Open-source software offers more control but worries about updates and vulnerabilities persist. Users find current user agreements unfair and lack agency due to complex legalese and "all-or-nothing" consent options. To improve the user experience, participants call for industry standards, clearer communication from manufacturers during adverse events, and regulations to discourage frequent releases of marginally updated devices.

4.1.1Ownership of the Device: Hardware vs Software

Participants' expectations about the ownership of IoT devices constituted a spectrum between total manufacturer control and total user control, with most citing that they saw it as a partnership between the manufacturer and the user, where the user was the owner of the hardware and leased the software from the manufacturer where their data was collected and stored.

> "When we talk about smart devices – for example, let's say Tesla, I own the car but if Tesla's software is not working at their end, I cannot actually start the car. So even if I have paid, I have the car physically in my garage, I cannot start it because the company might not have the software working at their end – so technically then, both the teams are the owner of that product." [J3]

The tangibility of the hardware allowed participants to have physical access to it. Participants said that they could maintain the device's hardware themselves but relied on the manufacturer to maintain the software within because it required specialised knowledge and skills which the participants did not have or wanted to learn themselves. Software maintenance was considered more complex than hardware and concerns around data security and privacy also deterred them to exercise more control over software. Technically confident participants who either had academic or professional training in software-related domains or were enthusiasts pushed for total user control through open-source software that gave them more flexibility to use the device as they wished. Other participants were worried about losing manufacturer support privileges if they tinkered with the software. Additionally, they expected their devices to be more vulnerable to cyberattacks if they operated on open-source platforms.

> "The other side of the coin is that if its opened up as open-source software that anyone can change [the software], you get a kind of anarchy which can work in some circumstances but equally also open up problems because people make changes that they don't fully understand the consequences of" [I5]

Participants also wanted to exercise greater control on managing data collected and stored by IoT devices using software and/or hardware mechanisms. At the same time, they did not know about the variety of data that could be collected by different kinds of IoT devices which also led them to overestimate the threats and underestimate the vulnerabilities associated with managing and repairing them.

Taking cue from the availability of both open-source software like Android OS and propriety software like iOS currently in the traditional ICT market, participants said that it ultimately depended on the user to choose how much control they want to assert. If they wanted more flexibility, they could choose open-source software and if they wanted more secure systems, they could go with propriety software systems.

4.1.2User Agreements and Lack of Agency

Participants intuitively said that they would revisit the user agreement signed with the manufacturer when they were faced with adverse scenarios such as sudden bricking of their IoT device due to losing manufacturer software support or losing smart functionalities because of infrastructural changes that drive the technology.

> "I would look at consumer protections in place for minimum standards around supporting this kind of stuff and warranties and that kind of thing." [I7]

User agreements were seen as instruments that can establish co-ownership of the IoT device, by setting user and manufacturer responsibilities and informing users about the device's functions, associated vulnerabilities, update schedules and support information.

However, existing user agreements were considered unfair by the participants even if it did include everything stated above. Firstly, they said that they couldn't exercise informed consent as they could not read so much information before consenting. Secondly, these agreements were designed as an "all-or-nothing" agreement as they did not allow the user to selectively consent to conditions they agreed with or withhold consent from conditions they did not agree with, thereby, forcing them to accept the manufacturer's conditions to use the IoT device they purchased.

> "…they [manufacturer] say we have your consent… but in general if we see the apps and… software updates, we don't really have a choice. We need to assent to be able to use a product. So, they are the dominating ones in the system, rather than us who is actually paying for the system and using it [sic]" [J3]

4.1.3Regulations and Benchmarking

As seen in section 4.1.1, participants accepted co-ownership of their IoT devices with the manufacturer and accepted that the latter had greater control on the maintenance of their devices. However, when probed with adverse scenarios participants saw a need for a regulatory layer in between to protect them and establish a fairer partnership.

Industry-wide collaboration and adoption of *open-standards* were seen as a method to allow other trusted parties to offer continuing support in the absence of the original manufacturer.

> "I recognise that not everyone may be comfortable with the open-source aspect, but it depends on the strength of the community that is supporting that software and if it's like a standard that has been around for a long time and is very well known and tested, [I would be comfortable using that device]" [I7]

Regulatory bodies were expected to outline standard operating procedures for the manufacturers to enable transparent, timely, informative, and actionable communication between the two parties, especially during critical events like a cybersecurity or privacy breach.

Participants also admitted that they had little incentive to repair their IoT devices as newer alternatives were readily available in the market. In this context, one participant suggested that the consumer tech sector could learn from the automobile sector which follows strict regulations for launching new generation of products. Similarly, dedicated bodies could regulate the frequent release of IoT devices by using benchmarking tools to ascertain significant changes from the previous version of the product. This, according to the participants, may nudge both the user and the manufacturer to maintain and support existing devices for a longer period while making upgrades more meaningful.

4.2 Tackling IoT Software Challenges

Participants deliberated on several considerations while addressing IoT software challenges. Firstly, they associated repair with hardware issues, while software problems were typically expected to be resolved through updates from manufacturers. Trust in manufacturers, therefore, was crucial in maintaining user confidence. Participants also negotiated for a reasonable period for continued software support and rejected support offered by post-official communities due to security and accountability concerns. Lastly, IoT devices were expected to maintain core functionalities independent of internet connectivity.

4.2.1Trusting the Original Manufacturer

Even though participants heavily relied on manufacturer support to tackle software challenges associated with their IoT devices, how the manufacturer responded to these challenges also helped build participant trust and determined if the participants would continue using the existing product and/or invest in their products in the future.

For example, if the manufacturer sent an automatic update to reverse the effects of a privacy breach in the participant's IoT device, they demanded the manufacturer to be transparent in their communications with the user.

> "I would need transparency to trust them – let me know about the breach, tell me the factors involved, tell me you resolved it, tell me what was fixed and tell me how you're stopping this from happening in the future. But tell me and don't push an update to fix it without telling me – it makes me question what else could be hidden from me – if there are more such issues in the system that I'm not aware of" [J2]

Conversely, participants were more likely to accept a manufacturer's actions if they had a high level of trust in the company itself. In the absence of trust, participants said that they would stop using the device, discard it or replace it with a device from a more trusted brand when faced with an adverse scenario. Manufacturers were expected to uphold good security standards and ensure privacy of the user, by default.

Lastly, if the manufacturer could not provide the participants with a solution, they expected them to compensate them for their losses either by offering them trade-in opportunities, discounts and/or reimbursements.

> "…I will have to evaluate the convenience of transitioning to a new device. If I am busy, I would probably not upgrade. It would be nice if the company could give me a trade-in service or offer its new devices on a discount. If security and privacy are actually really important concerns for me, and if I believe they are a crucial part of my daily life, then I may have to upgrade." [A2]

4.2.2Negotiating a Reasonable Period for Continued Software Support

The expectation of a reasonable period of software support was dependent on the type of IoT device. For example, a smart washing machine was expected to be supported for much longer than a smart speaker but lesser than a connected car.

> "I think the years of support depends on the device type – for example smart phones are 2-3 years, washing machines should at the very least be 5 years; I mean the contracts around smartphones are 2 years and I've replaced my smartphones around every 2 years. For a washing machine, ideally, you'd have it for 15-20 years but there is a general acceptance that companies cannot continue to roll out updates for devices that are tens of years old – I would definitely expect it to be more than a smartphone!" [I7]

They also expected a smart washing machine would have a shorter life than a traditional washing machine as the IoT device had embedded software on it as they believed that fast paced technological development and innovation led to technological devices becoming outdated faster and disallowed companies to keep supporting them for longer periods as newer software could not run on old hardware. "Smart" features on these devices made up for these shorter lifespans for them.

However as seen in section 4.1.3, participants also expected manufacturers to also make meaningful changes to products to justify these short lifespans. Even if the manufacturer could not push new feature updates on their smart devices, participants argued for longer, if not unlimited security updates for their devices.

> "For me, it depends on the kind of updates that would stop. If it's just losing feature updates, then realistically, what more can you add to a smart fridge after just 2 years? Also, what more can a smart washing machine do what I cannot do using my phone. So, if the features that are currently on the device are working, then I would not really upgrade." [A1]

In the absence of such support however, participants said that depending on the emotional or utilitarian value the device brings to their lives and the severity of risks it poses to their privacy and security, they would either choose to replace it, continue using it despite being vulnerable or take it offline.

4.2.3Lacking Trust in Post-official Communities

Participants did not trust post-official communities to continue maintaining software on their IoT devices in the absence of manufacturer support. They were worried about compromising their data, privacy, and security if they sought solutions from unofficial sources. This fear was exacerbated for IoT devices as they could be hacked to collect, steal, and manipulate various kinds of data from the user.

> "…I think in the past I would've [approached post-official communities] when the devices we had were not internet connected but now I wouldn't. I used to put custom firmware on my MP3 players and things like that, but I couldn't risk doing that on something that is connected to the internet" [I7]

Even though participants could use fixes and patches offered by these communities at their own volition, a lack of accountability and/or redressal mechanisms also deterred them from approaching them.

While participants said that a certification or accreditation of such groups from a credible source may improve their trust in these communities, they would always seek assistance from manufacturer-recognised/supported groups as they were safe, specialised, and accountable.

> "Third-party option makes me feel vulnerable – I feel that at every point in time the manufacturer should be responsible for the product, services and maintenance." [J1]

Also, from the outset participants maintained that the software was the manufacturers' expertise. For them to maintain the devices themselves with the help of post-official communities, they understood that they too would need to understand the software, which they did not want to do.

4.2.4Making IoT Devices Internet Independent

Participants were asked if the internet-enabled smart features on their IoT devices constituted as the core functionality of the device or was it a unique feature added to a traditional device. They were also asked if they would consider using their IoT devices without using these features in the absence of continued manufacturer support for the software as they said that they could in section 4.2.3.

According to their responses, IoT devices should provide the basic functionality offered by its traditional version. For example, a smart bulb should first be a bulb that can provide luminescence when required and then offer smart features such as remote control, lighting conditions, scheduling etc. Doing so could allow them to continue using the device safely when faced with certain software challenges such as losing software support or having their IoT device compromised.

> "My assumption is that the car still functions as a regular car, just without the stuff [smart services] that I was previously paying for." [G2]

However, some participants did not accept using an IoT device independent of its smart features as a suitable solution.

> "That's not really cool because how do you get a smart device and then it is no longer smart – it defeats the aim of the purchase." [J1]

Additionally, manufacturers were expected to design multiple ways to connect a device to the internet such that if one path became unavailable, they could use another one to achieve the same function. For example, when 3G services were rolled back in the US, participants said that connected cars should have leveraged existing infrastructure such as Bluetooth and mobile phones to maintain their functionalities instead of shutting their smart services and pushing consumers to purchase new cars.

4.3 Repair for the Reuse of IoT

The buying and selling of used IoT devices are complicated by differences in legal, technological, and cultural practices in different parts of the world. Lacking technological support and data-related concerns resulted in a lack of trust in previously used IoT devices amongst the participants in the, especially in the absence of manufacturers' support extended to second-hand devices.

4.3.1Data Interactions Underlying IoT Repair

While considering giving away their IoT devices, participants highlighted data-related concerns or lack thereof. While one participant stated that owning a smart device meant they did not worry as much about their personal data, another stated that they had no idea what types of data the gadget could store and process, thus they were not worried. Reset functions on IoT devices assured some participants that they could safely part-ways with their devices.

> "I don't think I would sell it I worry about the data that is still on them and probably seeing some of these other devices if they keep your login details on there or they've signed you into a service in the past and you're still logged in, the new person can potentially access it. It would worry me. It would be good if a device had a secure wipe button so you can know that it is okay to resell it. If I didn't have that then I would be quite hesitant to do it." [I2]

Seemingly Tangible Interactions. Participants said that they would reset their IoT devices before giving them away. Conversely, they also said that they would give away their devices only if they could reset it as seen in section 4.3.1.

> "…I would probably reset it before I sell. I think we do that every time we change our phone or something like that." [J2]

They preferred using multiple methods of resetting a device like using physical buttons or in-app reset options. Irrespective of the mechanism used, they expected the interface to confirm the success of their action after the reset by reverting to its original state.

> "The company can give you instructions on how to safely wipe the device... it's going to clear all information...remove every single thing...it's basically new...and then the new user can use it... Just making sure that you have the physical confirmation that everything is gone. I'm safe." [G2]

Participants also explained that sometimes they did not know that they needed to reset because they were not aware of the kinds of data being collected by an IoT device like a smart bulb. They said, they could benefit from timely messages or nudges to reset their device before they gave it away. They also wished for ways to protect their data afterwards if they failed to reset it.

Intangible Data Interactions (Data and Device vs Data and Accounts). However, participants' responses also revealed that data management may not be as tangible as they expected it to be and revealed more complicated aspects of account management and data portability. For example, it was unclear if the user could give away the device but hold onto the data generated by them. There was a lack of range of perceptions present here.

> "Most of the companies, when they employ a security camera, all the data is overridden after a certain amount of time, and this deleted. So, the thing is there is an app where you can see all your recordings, right? Even if you are selling the device, you don't really sell the data. It is not on the camera, and nobody should be able to access it because generally people have to sign in to access your data." [A2]

4.3.2Demanding Greater Manufacturer Support for Second Users

Even though participants were open to giving away their IoT devices for altruistic and/or economic reasons, they were not confident in purchasing second-hand devices for themselves as there were no guarantees of quality or function associated with them in the absence of manufacturer support. They expected the re-sellers to play the manufacturer's part and ensure that the device was set properly for a new user and provide broad support with issues around setting up the device.

> "I don't think I would have bought a second-hand device – if you do, you're going to have such problems – if it is still supported by the manufacturer, then you should be able to get assistance from the manufacturer – if not, you're on your own – really not much you can do" [I5]

Participants shared that if manufacturers recognised that their devices were being reused and designed them with the intention of reusability, then it would be easier for people to adopt second-hand IoT devices.

> "I recently bought a PlayStation, and it was factory reset and I was the new user and all the older accounts had been cleared off and it just made the whole thing a lot easier. Manufacturers should recognise and prepare their devices such that they could be resold and have a process in place." [I7]

Manufacturer support was especially important for the participants in cases where they encountered difficulties in resetting the device due to protective mechanisms such as Factory Reset Protection (FRP) and Multi-Factor Authentication (MFA) being used. While acknowledging that these measures were taken to protect the previous owners' privacy and existing challenges in validating the legality of device transfers as seen in section 3.4., participants believed that only manufacturers could implement systems to balance these competing demands.

> "If your device is stolen and someone else requests that this is the case, and the other previous owners' item is there. So, then he will have the power to reset it. It is a privacy concern, honestly." [A2]

As for the participants, they would like to always know about the accounts linked to their devices such that they can remove any old accounts previously linked to the device to protect their data.

5 DIscussion

All the findings reflect the perspective of the users. Based on these findings, we highlight three key sets of stakeholder focused recommendations for IoT design that embodies repairability. These are IoT related *user challenges* (that include data interactions, internet independence, privacy, and security) which call for a revision in the *role of the manufacturers* and a need for better support from *regulatory authorities*.

5.1 IoT-Specific User Challenges Associated with Repair

This section highlights three key challenges related to maintaining and repairing current IoT devices, namely, lacking usable privacy and security controls, uncertainties in repair and data interactions and a call for adopting an offline-first approach for IoT design.

5.1.1Privacy and Security as Barriers to Software Repair

A lack of trust in "unofficial" software tinkering due to concerns around security and privacy hindered users in our study from engaging in software repair practices. Only IoT device manufacturers were expected to maintain and repair their devices as they were seen as experts of the software being used and could be held accountable if things went wrong. Users did not trust themselves or post-official communities to maintain and repair the software as they believed such tinkering would make the device, and by extension themselves, more vulnerable to privacy and security risks. In fact, they would rather continue using devices that had been abandoned by the manufacturer, instead of engaging with independent software repair practices, even if that meant being vulnerable to security risks because of losing software support.

When considering IoT use, the users' ability to act, verify or enforce data privacy and security, is limited due to their assumption that their privacy is protected (owing to their trust in IoT device manufacturers) [89] and the (lack of) controls provided to them. [15] IoT manufacturers however see security and privacy as technical issues which are complicated by legal requirements and consider them separate from the domain of HCI. [11] Researchers have previously shown that user's trust in smart technology can be broken by unkept promises and errors that can cause rapid decline in its usage and even result in abandonment of certain systems. [86] Prior research has also demanded for greater usable privacy and security controls for household IoT devices that are context-aware and dynamic. [12, 15] However, these studies have primarily focused on enhancing usability of privacy and security interactions during the use-phase of IoT devices whereas the need for making such interactions available and usable to users in events of breakdown and repair is yet to be responded to.

Manufacturers have taken steps in this direction by introducing user-friendly "maintenance modes" for their non-IoT offerings such as smartphones, which disallow repairers from accessing user data and protecting their privacy during repair activities. [130, 131] However, these functions have usability problems of their own and lock-in users to utilise repair services from authorised service centres only and do not address issues related to software maintenance and repair.

Extending the scope of current repair responses and exploring the usability challenges prevalent here are challenges the HCI community is well-positioned to take up.

Hence, identified here is a need for designing interactions that enable secure interactions, for people with technology. Also, seen here is the need for interactions of people with people through post-official user communities and users with the manufacturers to enhance trust in these relationships. Research shows that post-official communities and their contributors should be better regulated [74] and communications from the manufacturer must be timely, informative and clear to activate users instead of limiting them. [132] With HCI's significant investment in usability research and CSCW, HCI would be a key contributor in both widening the scope of usable privacy and security to include the aforementioned unique challenges of IoT repair and also in unpacking the complex interactions embodied within multi-stakeholder communities required to foster increased repairability for IoT devices.

5.1.2Unclear Data Interactions

Users lack awareness, understanding and knowledge of the kinds of data collected, stored, used and shared by their IoT devices. [82] They lacked clarity about whether the data was being stored on the device or the cloud or both, how reset mechanisms worked and questioned if they worked at all. Such lack of awareness and control shaped their behaviour towards IoT devices, where they either overestimated the threats or underestimated the vulnerabilities associated with different devices. Other researchers too have found that expectations of threats and vulnerabilities were more pronounced for audio-visual (AV) IoT devices such as security cameras versus non-AV IoT devices such as smart bulbs. [89]

Users demanded greater data controls to manage their data streams during the use phase of their IoT devices so that they could familiarise with the extent of their data being captured to make better assessments and adjust their threat perceptions when passing on their device to another person. Unclear data interactions and incorrect de-ownership practices were seen to expose first users' data to bad actors [21] and/or block second users to access the functions of the device due to security mechanisms either built-in by design, such as FRP or mandated by laws, such as in cases of theft.

Despite existing offerings of data management controls by the manufacturers, these observations suggest that current household IoT devices fail at two out of three principles of Human-Data Interaction (HDI) [56], namely, 'data legibility' and 'agency through control' when considering use and reuse of IoT devices. [127] The HCI community being the foundation for HDI itself, calls to be the enabler for exploring contextualised studies [20] focused on maintainability and repairability where these HDI principles can be realised to contribute to better maintainability and repairability in IoT design. This operationalisation in turn also becomes a contribution to the fledgeling HDI domain [14, 53, 66] in establishing a more nuanced understanding of legibility and agency that is inclusive of device repair and sustainability, concerns that HDI as a knowledge stream currently fails to acknowledge.

5.1.3Making IoT Internet Independent

The unique selling point of IoT devices are the "smart" features they offer to the users over their non-IoT versions. While users preferred to utilise the IoT device to its full capacity, there was also the want for these devices to not be entirely dependent on the internet for functioning. For example, users wanted to take their devices offline to mitigate security risks in the event of a larger cyber-attack [112], or if the manufacturer abandoned the software on the device. [96] However, many individual IoT devices need an active internet connection to function at all. [25]

Users also discount the lifespan and the huge cost of an IoT device because of the "smart features" it offers and accepts the obsolescence that comes with "tech" products as a by-product of innovation. However, dumber devices tend to last much longer than their "smarter" counterparts and are more resilient to obsolescence caused by software and internet related issues. [79]

Here, designers need to adopt an offline-first approach [133] for the design of IoT devices based on the 'principle of baseline utility'. [39] This would manifest as the user having control over the core function they bought, with or without updates, where being connected offers them a progressive enhancement to the functioning of the device. This includes having physical fallbacks to using the device and have an option to opt-in for over-the-air updates. Such mechanisms would enable and empower users to continue using their IoT devices even in the absence of a software infrastructure that is broken due to the reasons discussed above. Investigating the myriad avenues of interaction between the user and the device that would enable said internet independence at different phases of a device's life cycle is an undertaking that is reserved for the HCI community owing to its expertise in people, technology, and their combined socio-technical interactions.

5.2 Revised Role of the Manufacturer

In this section, firstly, we explore how the current concept of IoT ownership is blurred and reimagine the relationship between the user and manufacturer to give users more agency. We then discuss how users' repair options are limited due to manufacturer (in)action and complex user agreements and close with a discussion on wider reforms needed to ensure continued security support for IoT devices.

5.2.1 "Managing" Co-ownership

The concept of ownership and liability within the realm of IoT was seen to be undefined. Users feel like co-owners of devices with manufacturers, maintaining the hardware while leasing the software that makes it smart. Furthermore, through internet connection manufacturers are allowed to stay connected with these products even after users purchase the device from them. Unlike traditional devices, users have a limited say in the functioning and life of the device, essentially operating at the manufacturers' discretion. [19, 39, 134] This tilts the balance of power significantly from the legal owner of the device (the user) to the 'real' owner of the device (the manufacturer), transforming IoT devices to something closer to services than goods. [19]

Users recognise this imbalance and demand for user-agreements to create a fair co-ownership. Since the inception of software services, licensing agreements and subsequent associated documents (e.g., privacy policies) have been riddled with extensive legalese and jargon spanning tens of thousands of lines with poor legibility and usability. [32, 85] These heavily favour the manufacturer. Users have no choice but to surrender control to gain even basic functionality [36, 81, 85], leaving them responsible for the hardware yet powerless over its software and potential malfunctions. Moreover, a change in user ownership through reuse further complicates the issue. [40]

This paradox demands designers, policy makers and researchers to define a new approach to IoT ownership, one that gives users more control and enable them to continue using their devices with increased agency. Concepts such as 'offline-first' and 'principle of basic utility' discussed in section 1.3., are also steps towards a fairer co-ownership of IoT devices. A detailed study of the tasks, contexts and interactions associated with this redefinition process is one that the HCI community is uniquely positioned to take up through bringing together multiple stakeholder viewpoints [34] to develop a complex yet practical interaction strategy that enables IoT repair within everyday mundane technology scenarios for the users.

5.2.2 Greater Support for Software Repair

It is clear by now that users are overwhelmingly dependent on the manufacturers to maintain and repair internet, software and data-related challenges associated with IoT devices. They do not have the ability, motivation, or both to undertake software maintenance. Moreover, in addition to the privacy, security and data-related concerns discussed in section 1.1., they fear taking external help from post-official repair communities also because manufacturers dissuade users to participate in unofficial software tinkering, leaving them with no recourse in the absence of manufacturer support. [6] Moreover, most communication from trusted sources recommend users to discard a device once the manufacturer support period ends. [132, 135]

These unique challenges associated with IoT repair require novel solutions to widen its support beyond the manufacturer, especially when users have little incentive to do so. Moreover, for such an approach to be successful users must be open and willing to look beyond manufacturer support. This calls for a provision of authorised permits and checks for DIY IoT solutions in the future, providing the benefit of safety, security, and nurturing user trust. [74] However, such a need for authorisation may dissuade organic communities to come up if the process is perceived to be too complicated or cumbersome. Additionally, any solution must also answer the question of accountability if things go wrong.

In [31], the “right to repair” software was reframed to the right to 1) revert to prior versions of the software 2) refuse updates 3) receive security updates for a longer time. Unlike hardware, software changes can be reversed and if manufacturers can allow users to rollback software to an earlier known safe state and communicate its effects in a transparent manner, users maybe more open to testing out different solutions available to them. In case of longer software updates, we need wider reforms to make the support period proportional to the expected lifetime of the device. The need to explore and understand the unique properties (time, medium, interactions etc.) of the various avenues of support that could be made available to the users to help with their IoT repair practice is a herculean task, one that the HCI could render significant support to through its expertise in user-centred research.

5.2.3Wider Reforms: Values, Ethos and Processes

Regular software updates are necessary for enabling new functions and patching security vulnerabilities in the device. While users understand that manufacturers’ business models limit them from supporting their IoT devices for eternity, they believe that the security patches should be offered to them for a reasonable period dependent on the device category. Many users also felt that the frequent release of tech products fuel manufacturers’ decisions to abandon old devices sooner than expected for economic gains. Limited software support also hinders the reuse of such devices by second users in the absence of continued security support.

Household IoT devices such as washing machines and televisions have been abandoned by big and established brands after just two years of support in the recent past. [45, 136] This situation is far worse for obscure and cheaper IoT offerings in the market. Regulations and users both have been demanding manufacturers to provide security patches for a period proportional to its estimated life. [132] Users urge manufacturers to cooperate to develop a common minimum viable and usable open management standard for different categories of products to streamline continued security support for its core functions. In the past, manufacturers have come together to develop common communication protocols like Matter [80] to improve interoperability between various IoT products. We believe that increased consumer and regulatory pressure could push them to extend the realm of design processes to include such aspects of maintainability and repairability. However, users must be assured that open standards are safe to use, as we discovered in our study that they are hesitant to "open" anything due to fears of greater vulnerability to attacks. This socio-technical sphere demands further multi-disciplinary attention that is user-centred. While HCI has recently started engaging with such socio-technical investigations around device repair [41] , the scope for extending this to include dimensions like software related issues, data complexities, social nuances, legal constraints etc. stands stark.

5.3 Embedding Repair in IoT Regulations

Lastly, we explore strategies to improve long-tern support (LTS) and repairability of IoT devices through the adoption of open standards and regulatory measures and put forth a case for integrating security, privacy, and repair-related legislations into a comprehensive code for IoT devices.

5.3.1Mandating Open Standards for LTS in IoT

Currently, initiatives like Matter (formerly known as Project CHIP) [104] aim to integrate and unify a fragmented IoT ecosystem in smart homes and existing standards like Zigbee [137] address communication but not software lifecycle. Manufacturers often prioritise closed systems, hindering long-term software support for IoT devices. [83] There is a need for a standard framework to guarantee long-term support (LTS) for different categories of IoT devices. While it is a challenging proposition, the EU has previously worked towards establishing open hardware standards for enabling users to use a single charging solution for all electronic devices. [95] Regulatory bodies can require manufacturers to work together to establish open standards to ensure continued support for devices which can no longer be supported by the manufacturer and thereby reducing the number of perfectly good devices entering landfills which would be discarded simply because of a lack of software support.

There have been some community efforts to bridge this gap: Open-source projects like Tasmota [3] and ESPHome [138] allow users to bypass manufacturer limitations with custom firmware. However, these solutions face trust deficit and are not supported by the manufacturers. Users are also hesitant due to potential security risks and/or the technical knowledge required to access them.

We envision a collaboration between the HCI community [1, 67, 84] with governments and regulatory bodies. The HCI community would contribute its expertise to enhance the usability and foster user trust in the design and implementation of open standards. Simultaneously, governments and regulatory bodies would mandate manufacturers to provide LTS [91] and actionable end of support plans for their products. [139] This would entail manufacturers collaborating to develop open standards that prioritise maintainability and repairability of IoT devices. For example, Fairphone recommends sources that users could visit to access security patches after the support period for the model ends in their final patch messages. [140]

Users also expressed a desire for regulatory bodies to check the frequent release of new IoT products that disincentivise manufacturers from maintaining their old IoT devices. According to them, manufacturers must prove that there has been a significant technological development in the product since the last release. Conversations around 'meaningful innovation' have been around in popular media for a while, especially in the context of smartphones where differences in each generation of products are getting harder to distinguish from one another. [141] Therefore, it would benefit both users and the environment if a standard for refresh cycles for IoT products could be developed, like in the case of the automobile sector, thereby pushing manufacturers to support their older devices for longer and simultaneously produce more robust household IoT devices.

5.3.2Reviewing Existing IoT Regulations

Regulatory bodies globally have produced direct or indirect laws and white papers to push manufacturers to adopt good security and privacy practices that also embody principles of maintainability and repairability in the design of IoT devices. EU/UK's new Cyber Resilience Act/Product Security and Telecommunications Infrastructure Act 2022 requires IoT manufacturers to communicate minimum software support period [98] or a 'best before' date [91]to the users in a clear and transparent manner that would aid users in making informed purchasing decisions. Preliminary studies have shown that such labels enable non-experts to intuitively compare various products available in the market and would indirectly incentivise manufacturers to provide LTS. [23, 55]

EU had also introduced benchmarking indices and labels depicting repair scores for various electronic products in 2021 but in its current design it does not include software and data-related aspects and focuses primarily on hardware aspects of repair. [13, 33, 64] However, impact studies on user behaviour in this scope have been largely inconclusive, with some studies revealing that users assume repair scores presuppose that the device is not durable, making them sceptical instead of purchasing them. [24, 28, 142]

Our study shows that maintainability and repairability of IoT devices is intricately linked with aspects such as security, privacy, data interactions associated with the software and internet connectivity embedded in its design. Users do not see repair in isolation but their decisions and abilities to repair IoT devices stem from their interactions with the technology, device manufacturers, independent communities and rules established by authorities. Therefore, the current legislative landscape would benefit from integrating various security, privacy, and repair related legislations under one comprehensive code for IoT devices that promise users secure, safe, usable, maintainable, repairable, and reusable products in the future. We open this multi-stakeholder, interdisciplinary call to the HCI community to bring together the various aforementioned players in this scheme to draw out a legislative response that is applicable for practitioners and viable for businesses while being inclusive of citizen wants and needs.

6 Conclusion

We are grappling with a severe global e-waste problem, which has been putting enormous pressure on the environment, the economy, and the society. Prolonging the lifecycle of digital devices through repair and reuse is the most effective way to reduce the e-waste streams. Despite the exponential increase in the number of IoT devices being used and discarded globally, current repair discourse has ignored these devices which suffer from double effects of hardware and software obsolescence and are vulnerable to cyberattacks via internet connectivity. Recent studies in HCI have recognised this knowledge gap and have opened discussions on hardware obsolescence. However, software related aspects have largely been overlooked. This study expands the scope of existing research on IoT repair to explore software and data-related challenges associated with maintainability and repairability in IoT design from a user perspective. It uses 5 textual scenarios which highlight diverse adverse instances to probe focus group discussions with IoT users. Our results explicate user perceptions of the role of key repair actors (users, manufacturers, and regulators) in upholding the maintainability and repairability of IoT devices, IoT specific software related challenges and concerns around the reuse of repaired devices. The paper concludes by uncovering user challenges (e.g., data interactions, internet independence, privacy, and security) that require a revision in the role of the manufacturer and pushes for better support from regulatory authorities. Further, it contextualises these recommendations within wider literature and highlights the unique position the HCI community holds as a key player in this future-facing, emergent problem space that calls for attention with urgency.

ACKNOWLEDGMENTS

This work is funded by the Engineering and Physical Sciences Research Council grant number EP/W024780/1 (Project name: Fixing the Future: The Right to Repair and Equal I-o-T). We would also like to extend our gratitude to participants, Donald Smith, James Robinson, and Joseph Saviour who consented to be acknowledged in this work.

REFERENCES

<bib id="bib1"><number>[1]</number>Shadi Abou-Zahra, Judy Brewer, and Michael Cooper. 2017. Web Standards to Enable an Accessible and Inclusive Internet of Things (IoT). In *Proceedings of the 14th International Web for All Conference* (*W4A '17*), 2017. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3058555.3058568

<bib id="bib2"><number>[2]</number>Syed Ishtiaque Ahmed, Shion Guha, Md. Rashidujjaman Rifat, Faysal Hossain Shezan, and Nicola Dell. 2016. Privacy in Repair: An Analysis of the Privacy Challenges Surrounding Broken Digital Artifacts in Bangladesh. In *Proceedings of the Eighth International Conference on Information and Communication Technologies and Development*, June 03, 2016. ACM, Ann Arbor MI USA, 1–10. https://doi.org/10.1145/2909609.2909661</bib>

<bib id="bib3"><number>[3]</number>Theo Arends. 2024. arendst/Tasmota. Retrieved April 26, 2024 from https://github.com/arendst/Tasmota</bib>

<bib id="bib4"><number>[4]</number>Mary Barreto, Diego Casado-Mansilla, Augusto Esteves, and Filipe Magno de Gouveia Quintal. 2022. Designing Smart Plugs for Interactivity and Energy Sustainability via a Survey and Thematic Analysis. In *Nordic Human-Computer Interaction Conference* (*NordiCHI '22*), 2022. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3546155.3546681</bib>

<bib id="bib5"><number>[5]</number>S. Bødker. 2000. Scenarios in user-centred design—setting the stage for reflection and action. *Interacting with Computers* 13, 1 (2000), 61–75. https://doi.org/10.1016/S0953-5438(00)00024-2</bib>

<bib id="bib6"><number>[6]</number>Christopher Boniface, Lachlan Urquhart, and Melissa Terras. 2024. Towards a right to repair for the Internet of Things: A review of legal and policy aspects. *Computer Law & Security Review* 52, (2024), 105934. https://doi.org/10.1016/j.clsr.2024.105934</bib>

<bib id="bib7"><number>[7]</number>Will Brackenbury, Abhimanyu Deora, Jillian Ritchey, Jason Vallee, Weijia He, Guan Wang, Michael L. Littman, and Blase Ur. 2019. How Users Interpret Bugs in Trigger-Action Programming. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, May 02, 2019. ACM, Glasgow Scotland Uk, 1–12. https://doi.org/10.1145/3290605.3300782</bib>

<bib id="bib8"><number>[8]</number>Christina Bremer, Harshit Gujral, Michelle Lin, Lily Hinkers, Christoph Becker, and Vlad C. Coroamă. 2023. How Viable are Energy Savings in Smart Homes? A Call to Embrace Rebound Effects in Sustainable HCI. *ACM J. Comput. Sustain. Soc.* 1, 1 (September 2023). https://doi.org/10.1145/3608115</bib>

<bib id="bib9"><number>[9]</number>Barry Brown, Alexandra Weilenmann, Donald McMillan, and Airi Lampinen. 2016. Five Provocations for Ethical HCI Research. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (*CHI '16*), 2016. Association for Computing Machinery, New York, NY, USA, 852–863. https://doi.org/10.1145/2858036.2858313</bib>

<bib id="bib10"><number>[10]</number>Jason Ceci, J. Stegman, and Hassan Khan. 2023. No Privacy in the Electronics Repair Industry. In *2023 IEEE Symposium on Security and Privacy (SP)*, May 2023. IEEE Computer Society, Los Alamitos, CA, USA, 3347–3364. https://doi.org/10.1109/SP46215.2023.10179413</bib>

<bib id="bib11"><number>[11]</number>George Chalhoub, Ivan Flechais, Norbert Nthala, Ruba Abu-Salma, and Elie Tom. 2020. Factoring User Experience into the Security and Privacy Design of Smart Home Devices: A Case Study. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, April 25, 2020. ACM, Honolulu HI USA, 1–9. https://doi.org/10.1145/3334480.3382850</bib>

<bib id="bib12"><number>[12]</number>George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. 2021. "It did not give me an option to decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (*CHI '21*), May 07, 2021. Association for Computing Machinery, New York, NY, USA, 1–16. https://doi.org/10.1145/3411764.3445691</bib>

<bib id="bib13"><number>[13]</number>Adèle Chasson. 2020. French repairability index: what to expect in January? *Right to Repair Europe*. Retrieved April 26, 2024 from https://repair.eu/news/french-repairability-index-what-to-expect-in-january/</bib>

<bib id="bib14"><number>[14]</number>Amir Chaudhry, Jon Crowcroft, Heidi Howard, Anil Madhavapeddy, Richard Mortier, Hamed Haddadi, and Derek McAuley. 2015. Personal data: thinking inside the box. In *Proceedings of The Fifth Decennial Aarhus Conference on Critical Alternatives* (*CA '15*), 2015. Aarhus University Press, Aarhus N, 29–32. https://doi.org/10.7146/aahcc.v1i1.21312</bib>

<bib id="bib15"><number>[15]</number>Chola Chhetri and Vivian Genaro Motti. 2022. User-Centric Privacy Controls for Smart Homes. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2 (November 2022), 349:1-349:36. https://doi.org/10.1145/3555769</bib>

<bib id="bib16"><number>[16]</number>Monica Chin. 2023. Schools bought millions of Chromebooks in 2020 — and three years later, they're starting to break. *The Verge*. Retrieved April 26, 2024 from https://www.theverge.com/2023/4/21/23691840/us-pirg-education-fund-report-investigation-chromebook-churn</bib>

<bib id="bib17"><number>[17]</number>Lorraine Conway. 2024. Right to Repair Regulations. (April 2024). Retrieved April 26, 2024 from https://commonslibrary.parliament.uk/research-briefings/cbp-9302/</bib>

<bib id="bib18"><number>[18]</number>Tim Cooper (Ed.). 2016. *Longer Lasting Products: Alternatives To The Throwaway Society*. Routledge, London. https://doi.org/10.4324/9781315592930</bib>

<bib id="bib19"><number>[19]</number>Bipin C. Desai. 2017. IoT: Imminent ownership Threat. In *Proceedings of the 21st International Database Engineering & Applications Symposium* (*IDEAS '17*), 2017. Association for Computing Machinery, New York, NY, USA, 82–89. https://doi.org/10.1145/3105831.3105843</bib>

<bib id="bib20"><number>[20]</number>Paul Dourish. 2018. What we talk about when we talk about context. *Personal Ubiquitous Comput.* 8, 1 (October 2018), 19–30. https://doi.org/10.1007/s00779-003-0253-8</bib>

<bib id="bib21"><number>[21]</number>Daniel J. Dubois, Roman Kolcun, Anna Maria Mandalari, Muhammad Talha Paracha, David Choffnes, and Hamed Haddadi. 2020. When Speakers Are All Ears: Characterizing Misactivations of IoT Smart Speakers. *Proceedings on Privacy Enhancing Technologies* 2020, 4 (October 2020), 255–276. https://doi.org/10.2478/popets-2020-0072</bib>

<bib id="bib22"><number>[22]</number>Wail El Hilali and Abdellah El Manouar. 2019. Towards a sustainable world through a SMART digital transformation. In *Proceedings of the 2nd International Conference on Networking, Information Systems & Security* (*NISS '19*), 2019. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3320326.3320364</bib>

<bib id="bib23"><number>[23]</number>Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor. 2023. Are Consumers Willing to Pay for Security and Privacy of IoT Devices? In *32nd USENIX Security Symposium (USENIX Security 23)*, August 2023. USENIX Association, Anaheim, CA, 1505–1522. Retrieved from https://www.usenix.org/conference/usenixsecurity23/presentation/emami-naeini</bib>

<bib id="bib24"><number>[24]</number>European Commission. Directorate General for the Environment. and Ricardo AEA Ltd. 2015. *The durability of products: standard assessment for the circular economy under the eco innovation action plan.* Publications Office, LU. Retrieved April 26, 2024 from https://data.europa.eu/doi/10.2779/37050</bib>

<bib id="bib25"><number>[25]</number>Brian Feldman. 2019. Can You Create a Smart Home Without the Internet? *Intelligencer*. Retrieved April 26, 2024 from https://nymag.com/intelligencer/2019/11/can-you-create-a-smart-home-without-the-internet.html</bib>

<bib id="bib26"><number>[26]</number>Despina Filippidou. 1998. Designing with scenarios: A critical review of current research and practice. *Requirements Engineering* 3, 1 (March 1998), 1–22. https://doi.org/10.1007/BF02802918</bib>

<bib id="bib27"><number>[27]</number>Joel Fischer, James Colley, Ewa Luger, Mike Golembewski, Enrico Costanza, Sarvapali Ramchurn, Stephen Viller, Ian Oakley, and Jon Froehlich. 2016. Session details: (IOT horizons) new horizons for the iot in everyday life: proactive, shared, sustainable. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct* (*UbiComp '16*), 2016. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3248595</bib>

<bib id="bib28"><number>[28]</number>Bas Flipsen, Conny Bakker, and Guus van Bohemen. 2016. Developing a reparability indicator for electronic products. In *2016 Electronics Goes Green 2016+ (EGG)*, 2016. 1–9. https://doi.org/10.1109/EGG.2016.7829855</bib>

<bib id="bib29"><number>[29]</number>Samuel Gibbs. 2018. Apple and Samsung fined for deliberately slowing down phones. *The Guardian*. Retrieved April 26, 2024 from https://www.theguardian.com/technology/2018/oct/24/apple-samsung-fined-for-slowing-down-phones</bib>

<bib id="bib30"><number>[30]</number>Dennis Giese and Guevara Noubir. 2021. Amazon echo dot or the reverberating secrets of IoT devices. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (*WiSec '21*), 2021. Association for Computing Machinery, New York, NY, USA, 13–24. https://doi.org/10.1145/3448300.3467820</bib>

<bib id="bib31"><number>[31]</number>Robert W. Gomulkiewicz. 2022. Considering a Right to Repair Software. Retrieved April 26, 2024 from https://papers.ssrn.com/abstract=4125608</bib>

<bib id="bib32"><number>[32]</number>Jens Grossklags and Nathan Good. 2007. Empirical studies on software notices to inform policy makers and usability designers: 11th International Confrence on Financial Cryptography and Data Security, FC 2007 and 1st International Workshop on Usable Security, USEC 2007. *Financial Cryptography and Data Security - 11th International Conference, FC 2007, and 1st International Workshop on Usable Security, USEC 2007, Revised Selected Papers* (2007), 341–355. https://doi.org/10.1007/978-3-540-77366-5_31</bib>

<bib id="bib33"><number>[33]</number>Lucas Rockett Gutterman. 2024. Failing the Fix (2024): Grading Laptop and Cellphone Companies on the Fixability of Their Products. *U.S.PIRG Education Fund*. Retrieved April 26, 2024 from https://publicinterestnetwork.org/wp-content/uploads/2024/02/FY24-Failing-Fix-Embargoed.pdf</bib>

<bib id="bib34"><number>[34]</number>Nicolai Brodersen Hansen, Christian Dindler, Kim Halskov, Ole Sejer Iversen, Claus Bossen, Ditte Amund Basballe, and Ben Schouten. 2020. How Participatory Design Works: Mechanisms and Effects. In *Proceedings of the 31st Australian Conference on Human-Computer-Interaction* (*OzCHI '19*), 2020. Association for Computing Machinery, New York, NY, USA, 30–41. https://doi.org/10.1145/3369457.3369460</bib>

<bib id="bib35"><number>[35]</number>Michelle Heacock, Carol Bain Kelly, Kwadwo Ansong Asante, Linda S. Birnbaum, Åke Lennart Bergman, Marie-Noel Bruné, Irena Buka, David O. Carpenter, Aimin Chen, Xia Huo, Mostafa Kamel, Philip J. Landrigan, Federico Magalini, Fernando Diaz-Barriga, Maria Neira, Magdy Omar, Antonio Pascale, Mathuros Ruchirawat, Leith Sly, Peter D. Sly, Martin Van den Berg, and William A. Suk. 2016. E-Waste and Harm to Vulnerable Populations: A Growing Global Problem. *Environmental Health Perspectives* 124, 5 (2016), 550–555. https://doi.org/10.1289/ehp.1509699</bib>

<bib id="bib36"><number>[36]</number>Alex Hern. 2015. I read all the small print on the internet and it made me want to die. *The Guardian*. Retrieved April 26, 2024 from https://www.theguardian.com/technology/2015/jun/15/i-read-all-the-small-print-on-the-internet</bib>

<bib id="bib37"><number>[37]</number>Marcel den Hollander, C.A. Bakker, and Erik Hultink. 2017. Product Design in a Circular Economy: Development of a Typology of Key Concepts and Terms: Key Concepts and Terms for Circular Product Design. *Journal of Industrial Ecology* 21, (May 2017). https://doi.org/10.1111/jiec.12610</bib>

<bib id="bib38"><number>[38]</number>Lara Houston, Steven J. Jackson, Daniela K. Rosner, Syed Ishtiaque Ahmed, Meg Young, and Laewoo Kang. 2016. Values in Repair. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, May 07, 2016. ACM, San Jose California USA, 1403–1414. https://doi.org/10.1145/2858036.2858470</bib>

<bib id="bib39"><number>[39]</number>Václav Janeček. 2018. Ownership of personal data in the Internet of Things. *Computer Law & Security Review* 34, 5 (2018), 1039–1052. https://doi.org/10.1016/j.clsr.2018.04.007</bib>

<bib id="bib40"><number>[40]</number>Md Sakib Nizam Khan, Samuel Marchal, Sonja Buchegger, and N. Asokan. 2019. chownIoT: Enhancing IoT Privacy by Automated Handling of Ownership Change. In *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data: 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, August 20-24, 2018, Revised Selected Papers*, Eleni Kosta, Jo Pierson, Daniel Slamanig, Simone Fischer-Hübner and Stephan Krenn (eds.). Springer International Publishing, Cham, 205–221. https://doi.org/10.1007/978-3-030-16744-8_14</bib>

<bib id="bib41"><number>[41]</number>Damla Kilic and Neelima Sailaja. 2024. User-Centred Repair: From Current Practices to Future Design. *International Conference on Human-Computer Interaction* (2024).</bib>

<bib id="bib42"><number>[42]</number>Jenny Kitzinger. 2005. Focus group research: using group dynamics. *Qualitative research in health care* 56, (2005), 70.</bib>

<bib id="bib43"><number>[43]</number>Konrad Kollnig, Siddhartha Datta, Thomas Serban Von Davier, Max Van Kleek, Reuben Binns, Ulrik Lyngs, and Nigel Shadbolt. 2023. 'We are adults and deserve control of our phones': Examining the risks and opportunities of a right to repair for mobile apps. In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency* (*FAccT '23*), 2023. Association for Computing Machinery, New York, NY, USA, 22–34. https://doi.org/10.1145/3593013.3593973</bib>

<bib id="bib44"><number>[44]</number>Richard A. Krueger. 2014. *Focus Groups: A Practical Guide for Applied Research*. SAGE Publications.</bib>

<bib id="bib45"><number>[45]</number>Andrew Laughlin. 2023. Smart products abandoned by big brands after just two years - Which? News. *Which?* Retrieved April 26, 2024 from https://www.which.co.uk/news/article/smart-products-abandoned-by-big-brands-after-just-two-years-aqf4o6V6VlE3</bib>

<bib id="bib46"><number>[46]</number>Sandra Laville. 2019. UK worst offender in Europe for electronic waste exports – report | Waste | The Guardian. *The Guardian*. Retrieved April 25, 2024 from https://www.theguardian.com/environment/2019/feb/07/uk-worst-offender-in-europe-for-electronic-waste-exports-report</bib>

<bib id="bib47"><number>[47]</number>Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. 2017. *Research Methods in Human-Computer Interaction*. Morgan Kaufmann.</bib>

<bib id="bib48"><number>[48]</number>Debra Lilley, Vanessa Bailey, and Fiona Charnley. 2013. Design for sustainable behaviour: a quick fix for slower consumption? (January 2013). Retrieved April 26, 2024 from https://repository.lboro.ac.uk/articles/conference_contribution/Design_for_sustainable_behaviour_a_quick_fix_for_slower_consumption_/9338642/1</bib>

<bib id="bib49"><number>[49]</number>Knud Lasse Lueth. 2020. State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time. *IoT Analytics*. Retrieved April 25, 2024 from https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/</bib>

<bib id="bib50"><number>[50]</number>John McCollough. 2009. Factors impacting the demand for repair services of household products: the disappearing repair trades and the throwaway society. *International Journal of Consumer Studies* 33, 6 (2009), 619–626. https://doi.org/10.1111/j.1470-6431.2009.00793.x</bib>

<bib id="bib51"><number>[51]</number>John McCollough. 2020. The impact of consumers' time constraint and conspicuous consumption behaviour on the throwaway society. *International Journal of Consumer Studies* 44, 1 (2020), 33–43. https://doi.org/10.1111/ijcs.12545</bib>

<bib id="bib52"><number>[52]</number>mdepypere. 2021. The French repair index: challenges and opportunities. *Right to Repair Europe*. Retrieved April 25, 2024 from https://repair.eu/news/the-french-repair-index-challenges-and-opportunities/</bib>

<bib id="bib53"><number>[53]</number>Yves-Alexandre de Montjoye, Erez Shmueli, Samuel S. Wang, and Alex Sandy Pentland. 2014. openPDS: Protecting the Privacy of Metadata through SafeAnswers. *PLOS ONE* 9, 7 (July 2014), e98790. https://doi.org/10.1371/journal.pone.0098790</bib>

<bib id="bib54"><number>[54]</number>David L. Morgan. 1996. Focus Groups. *Annual Review of Sociology* 22, Volume 22, 1996 (August 1996), 129–152. https://doi.org/10.1146/annurev.soc.22.1.129</bib>

<bib id="bib55"><number>[55]</number>Philipp Morgner, Christoph Mai, Nicole Koschate-Fischer, Felix Freiling, and Zinaida Benenson. 2020. Security Update Labels: Establishing Economic Incentives for Security Patching of IoT Consumer Products. May 01, 2020. IEEE Computer Society, 429–446. https://doi.org/10.1109/SP40000.2020.00021</bib>

<bib id="bib56"><number>[56]</number>Richard Mortier, Hamed Haddadi, Tristan Henderson, Derek McAuley, and Jon Crowcroft. 2014. Human-Data Interaction: The Human Face of the Data-Driven Society. https://doi.org/10.2139/ssrn.2508051</bib>

<bib id="bib57"><number>[57]</number>Jasmin Niess. 2022. Qualitative Research Methods in HCI. University of Oslo. Retrieved April 26, 2024 from https://www.uio.no/studier/emner/matnat/ifi/IN2020/h22/timeplan/08-hci-methods.pdf</bib>

<bib id="bib58"><number>[58]</number>Jon Porter. 2019. Used Nest cameras had bug that let previous owners peer into homes. *The Verge*. Retrieved April 26, 2024 from https://www.theverge.com/2019/6/20/18692741/google-nest-cam-security-flaw-wink-second-hand-pre-owned-spying-privacy</bib>

<bib id="bib59"><number>[59]</number>J. Preece, H. Sharp, and Y. Rogers. 2015. *Interaction Design: Beyond Human-Computer Interaction*. Wiley. Retrieved from https://books.google.co.uk/books?id=n0h9CAAAQBAJ</bib>

<bib id="bib60"><number>[60]</number>Marina Proske and Melanie Jaeger-Erben. 2019. Decreasing obsolescence with modular smartphones? – An interdisciplinary perspective on lifecycles. *Journal of Cleaner Production* 223, (2019), 57–66. https://doi.org/10.1016/j.jclepro.2019.03.116</bib>

<bib id="bib61"><number>[61]</number>Heather A. Rogers, Pauline Deutz, and Tomás B. Ramos. 2021. Repairing the circular economy: Public perception and participant profile of the repair economy in Hull, UK. *Resources, Conservation and Recycling* 168, (2021), 105447. https://doi.org/10.1016/j.resconrec.2021.105447</bib>

<bib id="bib62"><number>[62]</number>Daniela K. Rosner. 2014. Making Citizens, Reassembling Devices: On Gender and the Development of Contemporary Public Sites of Repair in Northern California. *Public Culture* 26, 1 (72) (January 2014), 51–77. https://doi.org/10.1215/08992363-2346250</bib>

<bib id="bib63"><number>[63]</number>Daniela K. Rosner and Morgan Ames. 2014. Designing for repair? infrastructures and materialities of breakdown. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing* (*CSCW '14*), February 15, 2014. Association for Computing Machinery, New York, NY, USA, 319–331. https://doi.org/10.1145/2531602.2531692</bib>
<bib id="bib64"><number>[64]</number>Laura Ruiz-Pastor and Jaime A. Mesa. 2023. Proposing an integrated indicator to measure product repairability. *Journal of Cleaner Production* 395, (2023), 136434. https://doi.org/10.1016/j.jclepro.2023.136434</bib>
<bib id="bib65"><number>[65]</number>Mostafa Sabbaghi and Sara Behdad. 2018. Consumer decisions to repair mobile phones and manufacturer pricing policies: The concept of value leakage. *Resources, Conservation and Recycling* 133, (2018), 101–111. https://doi.org/10.1016/j.resconrec.2018.01.015</bib>
<bib id="bib66"><number>[66]</number>Neelima Sailaja, Andy Crabtree, James Colley, Adrian Gradinar, Paul Coulton, Ian Forrester, Lianne Kerlin, and Phil Stenton. 2019. The Living Room of the Future. In *Proceedings of the 2019 ACM International Conference on Interactive Experiences for TV and Online Video* (*TVX '19*), 2019. Association for Computing Machinery, New York, NY, USA, 95–107. https://doi.org/10.1145/3317697.3323360</bib>
<bib id="bib67"><number>[67]</number>Jibran Saleem, Mohammad Hammoudeh, Umar Raza, Bamidele Adebisi, and Ruth Ande. 2018. IoT standardisation: challenges, perspectives and solution. In *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems* (*ICFNDS '18*), 2018. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3231053.3231103</bib>
<bib id="bib68"><number>[68]</number>Carsten Schulte, Jessica Krüger, Andreas Gödecke, and Ann-Katrin Schmidt. 2018. The computing repair cafe: a concept for repair cafes in computing edcuation. In *Proceedings of the 13th Workshop in Primary and Secondary Computing Education* (*WiPSCE '18*), 2018. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3265757.3265781</bib>
<bib id="bib69"><number>[69]</number>Kristin Scott and S. Weaver. 2014. Repair or Not to Repair: What Is the Motivation? *Journal of Research for Consumers* 26, (January 2014).</bib>
<bib id="bib70"><number>[70]</number>Satyajit Sinha. 2023. State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally. *IoT Analytics*. Retrieved April 25, 2024 from https://iot-analytics.com/number-connected-iot-devices/</bib>
<bib id="bib71"><number>[71]</number>Monique Sonego, Márcia Elisa Soares Echeveste, and Henrique Galvan Debarba. 2022. Repair of electronic products: Consumer practices and institutional initiatives. *Sustainable Production and Consumption* 30, (March 2022), 556–565. https://doi.org/10.1016/j.spc.2021.12.031</bib>
<bib id="bib72"><number>[72]</number>Akash Sriram and Akash Sriram. 2023. Microsoft ending support for Windows 10 could send 240 mln PCs to landfills - report. *Reuters*. Retrieved April 26, 2024 from https://www.reuters.com/technology/microsoft-ending-support-windows-10-could-send-240-mln-pcs-landfills-report-2023-12-21/</bib>
<bib id="bib73"><number>[73]</number>Michael Stead. 2016. A Toaster For Life: Using Design Fiction To Facilitate Discussion On The Creation Of A Sustainable Internet of Things. June 25, 2016. . https://doi.org/10.21606/drs.2016.455</bib>
<bib id="bib74"><number>[74]</number>Michael Stead and Paul Coulton. 2017. HealthBand: Campaigning For An Open and Ethical Internet of Things Through An Applied Process of Design Fiction. In *Cumulus REDO Conference 2017 Proceedings*, May 31, 2017. . Retrieved from https://www.researchgate.net/publication/326635160_HealthBand_Campaigning_For_An_Open_and_Ethical_Internet_of_Things_Through_An_Applied_Process_of_Design_Fiction</bib>
<bib id="bib75"><number>[75]</number>Michael Stead, Paul Coulton, and Joseph Lindley. 2019. The Future Is Metahistory: Using Spime-based Design Fiction As A Research Lens For Designing Sustainable Internet of Things Devices. September 02, 2019. .</bib>
<bib id="bib76"><number>[76]</number>Michael Stead, Paul Coulton, Joseph Lindley, and Claire Coulton. 2019. *Little Book of Sustainability for the Internet of Things*. ImagineLancaster, Lancaster University. Retrieved April 26, 2024 from https://petras-iot.org/wp-content/uploads/2020/10/Little_Book_of_Sustainability_for_the_Internet_of_Things.pdf</bib>
<bib id="bib77"><number>[77]</number>Michael Stead, Matthew Pilling, Thomas Macpherson-Pope, and Paul Coulton. 2023. The Repair Shop 2049: Co-Designing Sustainable and Equitable Transitions for Smart Device Repair with and for Local Communities. In *5th Product Lifetimes And The Environment Conference Proceedings*, May 31, 2023. . Retrieved from https://www.plateconference.org</bib>
<bib id="bib78"><number>[78]</number>Hamed Taherdoost. 2016. Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research. *International Journal of Academic Research in Management (IJARM)* 5, (2016). Retrieved July 26, 2024 from https://hal.science/hal-02546796</bib>
<bib id="bib79"><number>[79]</number>Susann Thoma and Fraunhofer IZM. Blame the software: Study reveals new risks to the longevity of electronic devices. Retrieved April 26, 2024 from https://techxplore.com/news/2023-04-blame-software-reveals-longevity-electronic.html</bib>
<bib id="bib80"><number>[80]</number>Jennifer Pattison Tuohy. 2023. 2023 in the smart home: Matter's broken promises. *The Verge*. Retrieved April 26, 2024 from https://www.theverge.com/23997548/matter-smart-home-2023-platforms</bib>
<bib id="bib81"><number>[81]</number>Tony Vila, Rachel Greenstadt, and David Molnar. 2004. Why We Can't Be Bothered to Read Privacy Policies. In *Economics of Information Security*, L. Jean Camp and Stephen Lewis (eds.). Springer US, Boston, MA, 143–153. https://doi.org/10.1007/1-4020-8090-5_11</bib>
<bib id="bib82"><number>[82]</number>Jessica Vitak, Michael Zimmer, Anna Lenhart, Sunyup Park, Richmond Y. Wong, and Yaxing Yao. 2021. Designing for Data Awareness: Addressing Privacy and Security Concerns About "Smart" Technologies. In *Companion Publication of the 2021 Conference on Computer Supported Cooperative Work and Social Computing* (*CSCW '21 Companion*), 2021. Association for Computing Machinery, New York, NY, USA, 364–367. https://doi.org/10.1145/3462204.3481724</bib>
<bib id="bib83"><number>[83]</number>Bahtijar Vogel and Dimitrios Gkouskos. 2017. An open architecture approach: towards common design principles for an IoT architecture. In *Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings* (*ECSA '17*), 2017. Association for Computing Machinery, New York, NY, USA, 85–88. https://doi.org/10.1145/3129790.3129793</bib>
<bib id="bib84"><number>[84]</number>Bahtijar Vogel and Rimpu Varshney. 2018. Towards designing open and secure IoT systems: insights for practitioners. In *Proceedings of the 8th International Conference on the Internet of Things* (*IOT '18*), 2018. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3277593.3277615</bib>
<bib id="bib85"><number>[85]</number>T. Franklin Waddell, Joshua R. Auriemma, and S. Shyam Sundar. 2016. Make it Simple, or Force Users to Read? Paraphrased Design Improves Comprehension of End User License Agreements. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (*CHI '16*), 2016. Association for Computing Machinery, New York, NY, USA, 5252–5256. https://doi.org/10.1145/2858036.2858149</bib>
<bib id="bib86"><number>[86]</number>Mikołaj P. Woźniak, Sarah Vöge, Ronja Krüger, Heiko Müller, Marion Koelle, and Susanne Boll. 2023. Inhabiting Interconnected Spaces: How Users Shape and Appropriate Their Smart Home Ecosystems. In *Proceedings of the 2023 CHI Conference on*

Human Factors in Computing Systems (*CHI '23*), April 19, 2023. Association for Computing Machinery, New York, NY, USA, 1–18. https://doi.org/10.1145/3544548.3581497</bib>
<bib id="bib87"><number>[87]</number>Rayoung Yang, Mark W. Newman, and Jodi Forlizzi. 2014. Making sustainability sustainable: challenges in the design of eco-interaction technologies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (*CHI '14*), 2014. Association for Computing Machinery, New York, NY, USA, 823–832. https://doi.org/10.1145/2556288.2557380</bib>
<bib id="bib88"><number>[88]</number>Haoxiang Yu, Jie Hua, and Christine Julien. 2021. Analysis of IFTTT Recipes to Study How Humans Use Internet-of-Things (IoT) Devices. In *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems*, November 15, 2021. ACM, Coimbra Portugal, 537–541. https://doi.org/10.1145/3485730.3494115</bib>
<bib id="bib89"><number>[89]</number>Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW (November 2018), 1–20. https://doi.org/10.1145/3274469</bib>
<bib id="bib90"><number>[90]</number>2020. *Electronic Waste and the Circular Economy*. Environmental Audit Committee, House of Commons, London, United Kingdom. Retrieved April 26, 2024 from https://committees.parliament.uk/publications/3675/documents/35777/default/</bib>
<bib id="bib91"><number>[91]</number>2021. Best Before Date Policy Brief: Device sustainability through long-term software support. *Privacy International*. Retrieved April 26, 2024 from https://privacyinternational.org/sites/default/files/2021-10/Best%20Before%20Report%20Final_0.pdf</bib>
<bib id="bib92"><number>[92]</number>2021. Inquiry report - Right to Repair. *Australian Government, Productivity Commission*. Retrieved April 26, 2024 from https://www.pc.gov.au/inquiries/completed/repair/report</bib>
<bib id="bib93"><number>[93]</number>2022. 3G Wireless Network Shutdown Means Your Car May Lose Automatic Crash Notification. *Consumer Reports*. Retrieved April 26, 2024 from https://www.consumerreports.org/cars/car-safety/3g-wireless-network-shutdown-impact-on-car-safety-a2215482633/</bib>
<bib id="bib94"><number>[94]</number>2022. Right to repair: the EU's actions to make repairs more attractive. *Topics | European Parliament*. Retrieved April 26, 2024 from https://www.europarl.europa.eu/topics/en/article/20220331STO26410/right-to-repair-eu-action-to-make-repairs-more-attractive</bib>
<bib id="bib95"><number>[95]</number>2022. Long-awaited common charger for mobile devices will be a reality in 2024 | News | European Parliament. Retrieved April 26, 2024 from https://www.europarl.europa.eu/news/en/press-room/20220930IPR41928/long-awaited-common-charger-for-mobile-devices-will-be-a-reality-in-2024</bib>
<bib id="bib96"><number>[96]</number>2023. The lights have been on at a Massachusetts school for over a year because no one can turn them off. *NBC News*. Retrieved April 26, 2024 from https://www.nbcnews.com/news/us-news/lights-massachusetts-school-year-no-one-can-turn-rcna65611</bib>
<bib id="bib97"><number>[97]</number>2023. Electronic waste (e-waste). *World Health Organisation*. Retrieved April 25, 2024 from https://www.who.int/news-room/fact-sheets/detail/electronic-waste-(e-waste)</bib>
<bib id="bib98"><number>[98]</number>2024. The UK Product Security and Telecommunications Infrastructure (Product Security) regime. *GOV.UK*. Retrieved April 26, 2024 from https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime</bib>
<bib id="bib99"><number>[99]</number>2024. Internet of Shit (@internetofshit) / X. *X (formerly Twitter)*. Retrieved April 26, 2024 from https://twitter.com/internetofshit</bib>
<bib id="bib100"><number>[100]</number>2024. What is the Internet of Things (IoT)? | IBM. Retrieved April 26, 2024 from https://www.ibm.com/topics/internet-of-things</bib>
<bib id="bib101"><number>[101]</number>2024. How HCI Integrates Speculative Thinking to Envision Futures * Journal of Futures Studies. *Journal of Futures Studies*. Retrieved April 26, 2024 from https://jfsdigital.org/how-hci-integrates-speculative-thinking-to-envision-futures/</bib>
<bib id="bib102"><number>[102]</number>2024. Right to repair: Making repair easier and more appealing to consumers | News | European Parliament. Retrieved April 25, 2024 from https://www.europarl.europa.eu/news/en/press-room/20240419IPR20590/right-to-repair-making-repair-easier-and-more-appealing-to-consumers</bib>
<bib id="bib103"><number>[103]</number>2024. About Us. *iFixit*. Retrieved April 26, 2024 from https://www.ifixit.com/about-us</bib>
<bib id="bib104"><number>[104]</number>2024. project-chip/connectedhomeip. Retrieved April 26, 2024 from https://github.com/project-chip/connectedhomeip</bib>
<bib id="bib105"><number>[105]</number>Waste from Electrical and Electronic Equipment (WEEE) - European Commission. Retrieved April 25, 2024 from https://environment.ec.europa.eu/topics/waste-and-recycling/waste-electrical-and-electronic-equipment-weee_en</bib>
<bib id="bib106"><number>[106]</number>How to Build a Circular Economy | Ellen MacArthur Foundation. Retrieved April 25, 2024 from https://www.ellenmacarthurfoundation.org/</bib>
<bib id="bib107"><number>[107]</number>CanRepair. Retrieved April 25, 2024 from https://www.canrepair.ca/</bib>
<bib id="bib108"><number>[108]</number>Australian Repair Network. Retrieved April 25, 2024 from https://www.griffith.edu.au/law-futures-centre/our-research/australian-repair-network</bib>
<bib id="bib109"><number>[109]</number>About - The Restart Project. Retrieved April 25, 2024 from https://therestartproject.org/about/</bib>
<bib id="bib110"><number>[110]</number>Home | Repair Café Aotearoa NZ. *Repair Café Aotearoa*. Retrieved April 25, 2024 from https://www.repaircafeaotearoa.co.nz</bib>
<bib id="bib111"><number>[111]</number>Join the campaign. *Right to Repair Europe*. Retrieved April 25, 2024 from https://repair.eu/join-the-campaign-2/</bib>
<bib id="bib112"><number>[112]</number>What is the Mirai Botnet? Retrieved April 26, 2024 from https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/</bib>
<bib id="bib113"><number>[113]</number>The circular economy in detail. Retrieved April 26, 2024 from https://www.ellenmacarthurfoundation.org/the-circular-economy-in-detail-deep-dive</bib>
<bib id="bib114"><number>[114]</number>Circulate products and materials. Retrieved April 26, 2024 from https://www.ellenmacarthurfoundation.org/circulate-products-and-materials</bib>

<bib id="bib115"><number>[115]</number>Electrical and Electronic Equipment: Ingredients for Successful Extended Producer Responsibility – Eunomia Research and Consulting. Retrieved April 26, 2024 from https://eunomia.eco/reports/electrical-and-electronic-equipment-ingredients-for-successful-extended-producer-responsibility/</bib>
<bib id="bib116"><number>[116]</number>Right to Repair 2023 Legislation. Retrieved April 26, 2024 from https://www.ncsl.org/technology-and-communication/right-to-repair-2023-legislation</bib>
<bib id="bib117"><number>[117]</number>Right to Repair India. Retrieved April 26, 2024 from https://righttorepairindia.gov.in/#!</bib>
<bib id="bib118"><number>[118]</number>Ecodesign and Energy Labelling Working Plan 2022-2024 - European Commission. Retrieved April 26, 2024 from https://energy.ec.europa.eu/publications/ecodesign-and-energy-labelling-working-plan-2022-2024_en</bib>
<bib id="bib119"><number>[119]</number>Waste from Electrical and Electronic Equipment (WEEE) - European Commission. Retrieved April 26, 2024 from https://environment.ec.europa.eu/topics/waste-and-recycling/waste-electrical-and-electronic-equipment-weee_en</bib>
<bib id="bib120"><number>[120]</number>Our impact - How do you make a fairer phone? *Fairphone*. Retrieved April 26, 2024 from https://www.fairphone.com/en/impact/</bib>
<bib id="bib121"><number>[121]</number>About Framework. *Framework*. Retrieved April 26, 2024 from https://frame.work/gb/en</bib>
<bib id="bib122"><number>[122]</number>Nokia G22 - A seamless smartphone experience. Retrieved April 26, 2024 from https://www.hmd.com/en_gb/nokia-g-22</bib>
<bib id="bib123"><number>[123]</number>Delayed smart meter programme fails to hit targets and secure public support - Committees - UK Parliament. Retrieved April 26, 2024 from https://committees.parliament.uk/committee/127/public-accounts-committee/news/197947/delayed-smart-meter-programme-fails-to-hit-targets-and-secure-public-support/</bib>
<bib id="bib124"><number>[124]</number>*Humanistic HCI*. Retrieved April 26, 2024 from https://link.springer.com/book/10.1007/978-3-031-02214-2</bib>
<bib id="bib125"><number>[125]</number>What are Smart Devices – Arm®. Retrieved April 26, 2024 from https://www.arm.com/glossary/smart-devices</bib>
<bib id="bib126"><number>[126]</number>Consumers make their homes smarter, with a focus on security. *Deloitte Insights*. Retrieved April 26, 2024 from https://www2.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey/2023/smart-home-industry-adoption-trend.html</bib>
<bib id="bib127"><number>[127]</number>Code of Practice for Consumer IoT Security.</bib>
<bib id="bib128"><number>[128]</number>3G Wireless Services Update. Retrieved April 26, 2024 from https://support.lexus.com/s/article/3G-Wireless-Services-10537</bib>
<bib id="bib129"><number>[129]</number>Berlin's New Airport Can't Switch Lights Off. *Sky News*. Retrieved April 26, 2024 from https://news.sky.com/story/berlins-new-airport-cant-switch-lights-off-10453083</bib>
<bib id="bib130"><number>[130]</number>Use Maintenance mode on your Galaxy phone or tablet. *Samsung Electronics America*. Retrieved April 26, 2024 from https://www.samsung.com/us/support/answer/ANS00091542/</bib>
<bib id="bib131"><number>[131]</number>Protect your data with the Maintenance mode. Retrieved April 26, 2024 from https://consumer-tkbdownload.huawei.com/ctkbfm/applet/simulator/en-gb00836096/index.html</bib>
<bib id="bib132"><number>[132]</number>Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security.</bib>
<bib id="bib133"><number>[133]</number>Offline IoT - Building Resilient Connected Devices without the Internet. *JSConf Budapest 2022*. Retrieved April 26, 2024 from https://jsconfbp.com/speakers/nick-hehr/</bib>
<bib id="bib134"><number>[134]</number>How the world will change as computers spread into everyday objects. *The Economist*. Retrieved April 26, 2024 from https://www.economist.com/leaders/2019/09/12/how-the-world-will-change-as-computers-spread-into-everyday-objects</bib>
<bib id="bib135"><number>[135]</number>Obsolete products. Retrieved April 26, 2024 from https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/obsolete-products</bib>
<bib id="bib136"><number>[136]</number>Privacy International research shows that smart device security updates fail to meet consumers' expectations | Privacy International. Retrieved April 26, 2024 from http://privacyinternational.org/press-release/4964/privacy-international-research-shows-smart-device-security-updates-fail-meet</bib>
<bib id="bib137"><number>[137]</number>What is Zigbee? | Definition from TechTarget. *IoT Agenda*. Retrieved April 26, 2024 from https://www.techtarget.com/iotagenda/definition/ZigBee</bib>
<bib id="bib138"><number>[138]</number>ESPHome. *ESPHome*. Retrieved April 26, 2024 from https://esphome.io/index.html</bib>
<bib id="bib139"><number>[139]</number>Copyleft Compliance Projects - Software Freedom Conservancy. Retrieved April 26, 2024 from https://sfconservancy.org/copyleft-compliance/vizio.html</bib>
<bib id="bib140"><number>[140]</number>Fairphone OS. *Support*. Retrieved April 26, 2024 from https://support.fairphone.com/hc/en-us/articles/9979180437393-Fairphone-OS</bib>
<bib id="bib141"><number>[141]</number>We Don't Need New Phone Launches Every Year. Here's Why. *CNET*. Retrieved April 26, 2024 from https://www.cnet.com/tech/mobile/why-we-dont-need-new-phone-releases-every-year/</bib>
<bib id="bib142"><number>[142]</number>Leveraging behavioural insights to design and test the repairability index in France. *The Behavioural Insights Team*. Retrieved April 26, 2024 from https://www.bi.team/publications/leveraging-behavioural-insights-to-design-and-test-the-repairability-index-in-france/</bib>

A APPENDICES

A.1 Textual Scenarios

Scenario 1: Malicious Updates and Cyberattacks

In 2016, the internet froze for several hours across the globe. Websites such as Netflix, Twitter, Instagram, and banking services such as Paypal and Deutsche Bank were brought to a creepy halt by a botnet – Mirai.

The weapon used? It sits in Chris's living room, on top of his 6-year-old's book-shelf – their indoor security camera. More than 600,000 vulnerable IoT devices were used to silently storm the server which hosted these websites. (How? Explained on the next page).

Chris never got to know.

- If you were Chris, would you have wanted to know if your camera was used in such an attack?

Three years later, the smartcam company introduced an automatic update which improved the device's security by introducing multiple levels of device authentication. This finally reversed the effects of the Mirai bot.

- Would you have continued using it after the issue had been resolved?

Chris and his family – his husband Rick, and their two daughters, Anne and Susie – continue using the smartcam which is an integral part of their home security system. At the same time, Mirai and its various strains continue to lurk in the webspace.

- Considering that you know the device had been used but was later fixed without your knowledge and is connected to other smart devices in the house, would you continue to use the devices?

Mirai attack, explained: Imagine you have smart devices like cameras or gadgets connected to the internet at your home. Some people don't change the default passwords on these devices, making them easy to guess. Now, the Mirai botnet was like a virtual army that searched the internet for these easy-to-guess passwords on devices worldwide. Once the botnet found such a device, it would tell another program to infect it with a kind of malicious software (malware). This infected device could then be controlled by a central server. When needed, all these infected devices could work together to overwhelm a website or online service, making it unavailable. This is called a distributed denial-of-service (DDoS) attack. When not causing trouble, these infected devices continued to search for more devices with weak passwords to spread the infection. So, in simple terms, the Mirai botnet was like a group of internet troublemakers using poorly protected devices to create chaos online.

Scenario 2: Limited Software Support

As a mature student, Amir had too many responsibilities: He was on top of his class during the day, a freelance designer at night and a single father of two through it all. However, he constantly felt pressed for time. On his way back from college one day, he noticed a peculiar billboard – Samsung was advertising for a washing machine!

Curious to find out more, he excitedly scoured for more information. Samsung SmartThings Washing Machine promised to allow him to control and monitor his laundry through his smartphone – from anywhere, all he had to do was put the clothes in the machine in the morning and forget about them. The machine would not only clean but also dry it for him before he got back home.

In fact, it worked so well for him that he slowly started building an ecosystem to automate his home tasks – the dishwasher came next, then the sensors and soon enough a microwave. Much like his mobile phone and laptop, these too received regular software updates – sometimes for introducing new features, sometimes for fixing bugs and mostly for regular maintenance. Since they were automatic, he did not really have to worry about them.

Two years later, he received a surprising e-mail:

(Email 1)

Hi Amir,

Thank you for being an integral part of our SmartThings family for the last 2 years. You have been a valued customer and therefore after careful evaluation, it has come to our attention that some of the older devices in your SmartThings ecosystem have reached the end of their service life and will no longer be able to receive software updates.

These include **SmartThings Washing Machine**, **SmartThings Microwave**

We understand the inconvenience this may cause and we apologise for any disruption it may have on your SmartThings experience. To continue enjoying the benefits of a seamlessly integrated smart home, we highly recommend considering our latest range of SmartThings devices, which feature advanced technology and improved functionality.

Should you require any assistance or have any questions, please do not hesitate to contact us. We are committed to assisting you in every way possible to ensure a seamless transition to our latest SmartThings devices.

Please note, unsupported devices can be vulnerable to cyberattacks.

Thank you for your continued support and understanding as we strive to provide you with the best smart home solutions.

Sincerely,
Samsung SmartThings Team

1. How would you respond in this situation? Why?

(Email 2)

Hi Amir,

Thank you for being an integral part of our SmartThings family. You have been a valued customer and therefore after careful consideration and evaluation, it has come to our attention that some of the older devices in your SmartThings ecosystem have reached the end of their service life. These include: **SmartThings Washing Machine**, **SmartThings dishwasher**

Due to limitations of the older hardware, in an increasingly fast paced technological landscape, it is getting harder to support these devices. We have constituted a new SmartThings unit to support older devices at a nominal cost of just 30 GBP per month per device. Please note, unsupported devices are vulnerable to attacks and therefore for your safety, they would no longer be functional.

We understand the inconvenience this may cause, and we apologise for any disruption it may have on your SmartThings experience. To continue enjoying the benefits of a seamlessly integrated smart home, we highly recommend considering our latest range of SmartThings devices, which feature advanced technology and improved functionality.

Should you require any assistance or have any questions, please do not hesitate to contact us. We are committed to assisting you in every way possible to ensure a seamless transition to our latest SmartThings devices.

Thank you for your continued support and understanding as we strive to provide you with the best smart home solutions.

Sincerely,
Samsung SmartThings Team

- How do you feel about this solution? Why?

(Email 3)

Hi Amir,

Thank you for being an integral part of our SmartThings family. You have been a valued customer and therefore after careful consideration and evaluation, it has come to our attention that some of the older devices in your SmartThings ecosystem have reached the end of their service life and will no longer be able to be updated or supported. These include: **SmartThings Washing Machine**, **SmartThings Microwave**

Your devices will continue to function, however internet connected services such as remote control and scheduling can no longer be accessed on the application.

We understand the inconvenience this may cause, and we apologise for any disruption it may have on your SmartThings experience. To continue enjoying the benefits of a seamlessly integrated smart home, we highly recommend considering our latest range of SmartThings devices, which feature advanced technology and improved functionality.

Should you require any assistance or have any questions, please do not hesitate to contact us. We are committed to assisting you in every way possible to ensure a seamless transition to our latest SmartThings devices.

Thank you for your continued support and understanding as we strive to provide you with the best smart home solutions.

Sincerely,
Samsung SmartThings Team

- How would you feel about this solution? Why?

At college, Amir lamented about the situation to his peers who asked him to reach out to other people who may have faced similar issues. He looked for support groups on Facebook and found a group of SmartThings users. There he found a post-official support group which consisted of community software developers who churned out bug fixes and software support for these abandoned devices. While it seemed like the better option, the groups disclaimer clarified that they were not associated with Samsung and therefore heeding advice and adopting practices was at the risk of the user.

- How would feel about this solution? Why?

Scenario 3: Changes In Supporting Infrastructure

Lexus is a luxury automaker brand that offers cars with internet connected services through its Enform Connect platform. Enform Connect is a mobile application which enables users to leverage the benefits of the internet with features like: The company uses cellular network like 3G/4G and 5G to communicate with the car and the mobile application of the user. For this they had installed a 3G cellular module in the cars. Similar to that on our mobile phones that we use to access internet. In 2022, Lexus announced that it is shutting down its services offered through 3G cellular network as cellular providers were dropping 3G for newer network technologies such as 4G and 5G. This would mean that cars that had 3G-enabled smart services discussed above, would no longer be operational. Lexus was not the only company affected by such a change in technology and infrastructure. Other major carmakers too had to cease their smart services due to this change.

1. Read the conversation below

   Claire: I just received a letter informing me that Lexus is doing away with all 3G Enform services in 2022. This includes remote start, safety destination and roadside services. A 70K vehicle and they're just going to delete a major feature of the vehicle? It is a service that I pay 250 GBP for I use it!

   Troy: Your Enform services run on a 3G cellular network. As the letter says, more and more cellular providers are dropping 3G networks (to evolve and support 4G and new 5G networks). As more 3G networks are phased out, Lexus would not be able to offer your particular Enform services nation-wide; and in the near future, as 5G becomes the norm, 3G networks will likely be dropped all together, everywhere!
2. How would you feel if you were Claire and how would you expect the problem to be resolved?
3. Probe: In reality, when designers are designing a smart device, they cannot foresee the technological advancements that may happen in the future. What could make the user more comfortable to continue using a product in such a situation?

Scenario 4: Software Ownership

On the corner of George Street, there is a house where the light never goes out.

In 2021, under the pressure of the looming economic crises since the pandemic, Renu was looking for ways to save money. Given the worsening situation on the Ukraine-Russia border, she understood that electricity and gas were going to become extremely expensive – and she had to find a more energy efficient solution for her house. That's when she came across Reflex Lighting Co., a lighting solutions company that developed and installed smart lighting systems which adapted to the ambient light – lower intensity with higher ambient light and higher intensity in places with lower ambient lighting.

This was especially helpful for her since her current house had ceiling lights installed that could either all switch on or all off – irrespective of where they were placed – close to the windows or at the far end of their house. What impressed her the most was that she had to do nothing to control them, it was all programmed in and while it was considerably costlier than traditional lighting systems – given the highly sophisticated software associated with it – she thought it would be worthwhile in the long run...and it really worked. Her bills halved from 165 GBP per month to just over 80 GBP. Not only that, but she also noticed that her eyesight got better because of this change! Things were great…until they weren't.

On September 24, 2022, the city centre had a massive power cut due to the Northern storm. For two hours, the streets went pitch black. When the power was restored, Renu saw all of her lights switch on, in all of their magnificent brightness and she could not turn them off.

Since the lighting system had failed, as a safety measure, the default position was to be on at all times. Unless she either took the 50 bulbs out manually or used circuit breakers to close sections of it, there were no manageable means of overriding this due to the proprietary nature of the lighting system.

1. How would you have tried to solve this problem?

She reached out to the original installer of the system – which it turns out had been sold multiple times in the last year. When she finally reached the new parent company, it took her even greater efforts to find someone familiar with the system installed at her house. After many weeks of efforts, she was provided an estimate of an excess of 7000 GBP to comparably replace the entire system.

Her next effort was to engage with a software consultant to explore whether it was possible to patch the system or code some ability to override the default with a simple timer or on/off switch of some sort. This was deemed not possible.

- In your opinion what would be a better way for the system to work?

Scenario 5: Resetting Problems in Second-Hand IoT

You have recently purchased a new smart speaker and are considering what to do with the old one.

1. How would you feel about selling/donating/giving away your old smart speaker? Why?
2. How would you go about selling/donating/giving away your old smart speaker?

You have recently purchased a second-hand smart speaker online. On connecting the smart speaker, you realise that the speaker is still connected to the old owner's account. You try to factory reset it by pressing buttons on it. It clears the data on the device, but it does not allow you to re-register due to security reasons. You try contacting the previous owner, but they have not responded in the past month.

1. How would you try to fix the situation?
2. In your opinion, what would be a better way for the system to work?

You recently sold your old indoor security smart camera online after having deregistered it from its application. One day, while using your smart home hub app, you notice that you can access the recordings of its new owners from your phone. You realise that it was because you had connected your camera to other smart devices at home through a common hub. The camera was therefore also registered on the hub's-application. Since the camera was deregistered from its old account, the new owner was able to sign up for a new account without any indication that the device was still associated with its old owner in any way.

1. If you were the old owner, what would you do?
2. If you were the new owner, how should this situation have been resolved?