Help Me Help You: Privacy Considerations for Third Party IoT Device Repair

Nathan Reitinger
University of Maryland

Weijia He
University of Southampton

Chelsea Bruno
University of Michigan

Susan Landau
Tufts University

Carl A. Gunter
University of Illinois at Urbana-Champaign

Mounib Khanafer
American University of Kuwait

Ravindra Mangar
Dartmouth College

Denise Anthony
University of Michigan

Abstract

Smart home devices are becoming increasingly complex and data-rich. The inevitable repair of these devices will be both difficult and privacy-sensitive. A “HandyTech”—a technician for home Internet of Things (IoT) system repair—has the potential to lower barriers to repair, but privacy questions remain: Are people willing to use a HandyTech to fix a broken home IoT device despite the inherent privacy risk (i.e., allowing a third party to access potentially sensitive IoT data)? We explore this question through a vignette-based, multi-factorial survey with a nationally representative sample of adults in the United States. We further ask whether types of devices (i.e., smart speakers, refrigerators, and CPAP machines) and factors adjacent to privacy and associated with the HandyTech’s work (i.e., scope of access, state-based licensing requirements, and transparency provisions) affect decisions to use or not use a HandyTech. We find that some demographic groups are more willing than others to use a HandyTech (e.g., younger age groups, those with children in the home). Current ownership of more types of smart devices increases willingness to use a HandyTech, while greater concerns over general IoT privacy decreases willingness to use a HandyTech. Device-specific perceptions also mattered, such that perceived urgency to fix is strongly associated with willingness to use a HandyTech, but concern over that device’s privacy is not. In addition, reduced scope of access and increased transparency by the HandyTech statistically increased willingness to use a HandyTech. In closing, we recommend takeaways that developers and policymakers can engage with to decrease privacy concerns and increase the adoption of third-party IoT repair.

Keywords

Smart Homes, IoT, Repair, Privacy

1 Introduction

It is estimated that three in five consumers in the United States will own a smart home device by 2025 [41]. Globally, the adoption of smart home technology is seen as imminent (even if some countries are expected to adopt the technology more quickly than others [19]). In fact, consumers may have a harder time purchasing a non-smart device than a smart device in the future [73].

The increased convenience, energy efficiency, and safety, however, do not come without a cost: Smart devices increase the complexity of the digital home [8], meaning more bugs, more errors, more vulnerabilities, and more privacy threats [87]. Complexity also makes it more difficult for a typical consumer to locate and repair a broken device. If a “dumb” lamp fails to turn on, it is most likely that the light bulb has run its course, warranting a simple replacement. If a smart lamp becomes unresponsive, it could be that the lamp’s Wi-Fi connection needs to be reset, or maybe the router itself has an issue, or maybe the user needs to re-log into the app controlling the lamp and update the app’s software or lamp’s firmware. IoT devices, unlike their non-smart counterparts, create a bevy of potential sources for error.

On top of this, although consumers may attempt to remedy smart home issues themselves, self-help in the smart world creates a variety of technical, legal, and social challenges [80]. For one, manufacturers of smart devices often seek protection from consumer tinkering by way of anti-right-to-repair agreements, barring consumers from even attempting repairs without voiding a warranty [33]. Consumers may also lack the technical skills or the time needed to diagnose and fix a smart device. Additionally, as devices may have multiple owners (e.g., a landlord and a renter), it can be socially troublesome to risk further breakage of a shared smart device by a non-expert consumer (e.g., “bricking” a smart refrigerator).

Finally, while some services do exist to aid with smart device repairs, these services are often tied to specific devices per manufacturer or retailer agreements, leaving consumers without a clear option for most devices and, even if the device qualifies for repair, the device may be out of warranty given particular types of failures or warranty shelf life. More importantly, even if the device is within warranty and repair or replacement is an option, these solutions nonetheless present a privacy concern (privacy here is considered to be a broad, contextually-based, social construct [88]). The repair of a device with potentially sensitive information on it presents a potential privacy invasion. Literature supports this proposition and even goes so far as to suggest that privacy invasions persist regardless of whether a company orchestrates or pays for a repair [1]. Willingness may be affected if the participant is, for example, so

Proceedings on Privacy Enhancing Technologies 2025(4), 216–235

https://doi.org/10.56553/popets-2025-0128

concerned about privacy as to abandon the repair or refuse to send a broken device with sensitive information on it to a shop for repair.

As prior work suggests, there may be a good solution to this problem: the HandyTech [**?**]. Just as it is common to call an electrician or a plumber to fix a difficult, risky, and skillful repair on an electrical or plumbing issue, consumers may seek a person skilled in IoT device repair. Prior work entertaining this problem considers the HandyTech to be "a technically skilled contractor who can set up, repair, debug, monitor, and troubleshoot home IoT systems [8]."

Although the prior work did provide a preview of the benefits and privacy implications of someone serving in this role, many questions remain. Who would hire a HandyTech? What demographic characteristics do these individuals possess, and what does that say about privacy [74]? Under what circumstances are people more or less likely to use a HandyTech? How willing are people to let a HandyTech fix particular devices—from those that are relatively mundane, like a smart speaker, to those that are more privacy-sensitive, like a smart medical device? What privacy protections should policymakers or developers consider for the HandyTech's role? We grouped these inquiries around three research questions:

RQ-1 - Who is willing to use a HandyTech?
RQ-2 - What factors (i.e., access scope, transparency, and licensing) influence the willingness to use a HandyTech?
RQ-3 - How does a device's privacy sensitivity and urgency-to-fix impact a participant's willingness to use a HandyTech?

We set out to answer these questions in a nationally representative ($n = 4,898$) vignette study conducted by YouGov in July 2024. Participants were randomly assigned to own one of three broken smart devices: a smart speaker, a smart refrigerator, or a smart continuous positive airway pressure (CPAP) machine. These devices were picked to provide a spectrum of privacy sensitivity and high-to-low urgency to fix: A smart CPAP machine is a life-saving health device that monitors sensitive health information, and is therefore likely highly private and urgent to fix; a smart refrigerator, on the other hand, may not contain sensitive information, but is likely urgent to fix in order to prevent food from spoiling; finally, a smart speaker is somewhat privacy-invasive, but likely presents less of an urgent need to fix.

A vignette described the role of a HandyTech in fixing these hypothetically broken devices, and participants were given two of three conditional factors: The scope of access a HandyTech has (i.e., more access may be more privacy-invasive); the HandyTech being licensed (i.e., whether state-based merits requirements for being a HandyTech affect willingness to use the HandyTech); and the level of transparency the HandyTech provided following a repair (i.e., either all actions the HandyTech took in repair were shared with the participant or none of the actions were shared). These factors represent action items for developers and policymakers in the third-party repair context. For example, if people are more willing to use a HandyTech when access scope is reduced, then a developer may find it fruitful to design access control mechanisms in the context of third-party device repairs. Likewise, if participants are more willing to use a HandyTech to fix a device when a receipt of all actions taken during a repair is provided, then policymakers or industry standards organizations may look to requiring this type of transparency by default, similar to how the auto repair industry has been pushed toward regulatory protections requiring transparency [32]. Finally, a policymaker may be interested in considering how an emerging HandyTech industry should be licensed, similar to the requirements for other highly technical repairs of products, such as auto-repair, which is inherently opaque to users and creates privacy or security concerns that are not easily addressed by individuals [32]. Afterward, participants were given a 5-point Likert question to determine how willing they were to use a HandyTech to fix their device.

We find that demographic groups, privacy-adjacent factors, and devices are all relevant in a participant's determination to use a HandyTech. Age, with younger participants being more willing to use a HandyTech, and current ownership of smart devices, with more devices associated with more willingness to use a HandyTech, were statistically significantly related to a participant's willingness to use a HandyTech. The factors of access scope and transparency were also significantly related to willingness, with less access by the HandyTech and more transparency about the HandyTech's actions making participants more likely to use the HandyTech. The type of device was also related to willingness to use a HandyTech, with the most urgent-to-fix devices (i.e., the CPAP and refrigerator) having a clear impact on willingness, but privacy had a less clear impact. In general, participants who were more privacy-sensitive about IoT data sharing were less likely to use a HandyTech.

The rest of this paper is organized as follows. In Section 2, we discuss the differences between traditional home appliances and smart home appliances, followed by the related work on smart home technologies, privacy, and repair. We then provide details on the methodology and data used to address our research questions in Section 3. In Section 4, we provide our findings and address additional analyses to test our research questions. We end with a discussion in Section 5.

2 Background and related work

In this paper, we investigate a particular type of third-party repair person, the HandyTech, a position we envision for a future where smart home devices are the norm and, as it is today, those devices break [8]. A HandyTech would serve a similar role as a plumber or electrician, but focuses on fixing IoT home devices. We aim to explore people's comfort and willingness to use a HandyTech, in turn shedding light on how participants perceive privacy in the context of third-party repairs. Our work touches on prior work in four different areas: smart home device challenges, privacy in the context of smart home devices, comfort in device repair, and competing considerations involving privacy choices.

2.1 Smart home device challenges

More and more devices are becoming "smart" and many of these devices are being used in the home [59]. From light bulbs to refrigerators to dishwashers, the proliferation of Internet-connected devices (i.e., IoT) is rapidly advancing. In global assessments of IoT adoption, more than half of all households had an IoT device, with some regions, like North America, having one or more smart devices in over 70% of all homes [49]. These smart devices can assist with the automation of tedious home tasks, safety functions, and the ability to manage the home remotely [25, 70, 79].

At the same time, for all of their convenience, these devices greatly increase the complexity of the home [24]. Adding Internet connectivity to a device also adds a host of complex networking protocols, software paradigms, and infrastructure [9, 13, 16, 23, 61, 63, 81, 83, 92, 93]. Together, this can cause problems in security, usability, abuse, functionality, and privacy [6, 26, 37, 62, 90]. Researchers have looked into each of these areas, focusing on automating security patches for smart devices, improving the usability of the devices, or canvassing privacy issues [11, 42, 86]. Here, we focus on a particular resource that can aid in many of these problems, a third-party expert who can patch security flaws, repair broken devices, or assist with privacy preferences.

2.2 Privacy for smart home devices

A large body of related work covers research on privacy concerns over smart home technologies, which range across many fields [18, 38, 40, 44, 56, 58, 65]. Studies focusing on privacy find that people's expectations of and concerns about privacy vary with social context [66], such as the type of data, the recipient of the data, the purpose of the data, and whom it benefits [12, 38, 40, 58, 65]. Depending on these contextual factors, people's comfort with data collection shifts [82]. Being less comfortable with data coming from more private spaces exemplifies the issue for a HandyTech, who necessarily works in the context of a home, where privacy is often at its zenith [21]. This can lead to a refusal to adopt certain devices like smart speakers [50], smart watches [55], or smart lights [45]. Some users, however, value the benefits offered by smart home technologies [50, 56, 72], and, where sufficient trust and well-justified purposes or general utility exist, users may even be willing to allow invasive data collection [44].

2.3 Comfort in device repair

Despite becoming much more prevalent in homes, smart home devices face challenges regarding repair. As pointed out by Sailaja et al., establishing repairability for smart home devices requires a joint effort from various disciplines, such as law, sociology, computer science, design, and more [80]. Beyond this, few researchers have investigated the repair issues of smart home devices from the perspective of a third-party repair person. However, researchers have looked into smartphone repair shops and the privacy implications behind them [4, 22, 36]. Prior studies show that the device repair industry lacks policies or standards to protect data residing on customers' devices [22, 36]. Ahmed et al. even found that some technicians may sell customers' data that they got through snooping [4]. On the other hand, Ceci et al. discovered that 33% of the broken devices they investigated were not repaired due to privacy concerns [22]. These findings could be easily generalized to the smart home contexts, where similar privacy challenges exist. Thus, more studies are needed on alleviating customers' privacy concerns when repairing their smart home devices.

2.4 Privacy decision making

Privacy decisions are not made in a vacuum. For instance, it is well documented that demographic attributes affect privacy choices [5, 74]. Another long line of literature has looked into the factors users weigh when making privacy-relevant choices. This literature is often grouped under the claimed "privacy paradox": the idea that users will make choices negatively affecting their privacy despite holding pro-privacy opinions. This paradox is not without direct application to smart home privacy. For example, researchers in IoT have looked at this paradox from a device adoption standpoint and found that despite privacy concerns, users still adopt IoT devices [54]. That point aside, researchers have also found clear connections to increased privacy concerns in the smart home context [96].

Critics of the claimed "paradox" are many and range in discipline [39, 46, 89]. The overall theme is that behavior may or may not be associated with particular attitudes toward privacy: When privacy is studied as a multidimensional concept [30], actual privacy choices versus hypothetical privacy choices are considered [2], people with heightened privacy preferences are studied in comparison [29] and the calculus of trade-offs is taken into account [53] the paradox is narrowed or deemed to not exist at all. In turn, the prevailing view of privacy decision-making is that it is complex and multidimensional—users make privacy-relevant decisions based on a variety of factors and personal beliefs. A user's decision negatively impacting privacy may not related to the user's overall attitude toward privacy, may be biased given an uninformed understanding of technology, may be reliant on alternative paths besides information sharing to protect privacy, or may be the result of fatigue, time pressures, or a prioritized utility in a specific context.

3 Methods

We set out to understand how receptive people are to the idea of using a third party to fix broken smart devices in their homes. Participants were given a hypothetical scenario involving a broken IoT device to which they were randomly assigned in a between-subjects[1] design: (1) smart speaker, (2) smart refrigerator, or (3) smart CPAP machine (see Appendix A for full vignette description). These devices were picked because each has unique characteristics that make the device more or less urgent to fix and more or less privacy-invasive. Below, we provide more details on why each device was picked.

3.1 Privacy and urgency-to-fix

We wanted to understand how privacy and urgency affect willingness to use a HandyTech. Addressing these properties (privacy and urgency to fix) would allow for more generalizable results (e.g., how to accommodate privacy concerns) and an improved understanding of how people feel about the privacy implications of third-party IoT repairs. One option to address these properties would have been to ask participants to imagine a scenario where a smart home is full of devices, and some of those devices are private, urgent to fix, or both. This scenario, however, lacks ecological validity and incorporates too many compounding and unknown factors that would make it difficult to glean takeaways from. Therefore, we instead picked devices—based on a literature review (see Section 3.3)—that were known to be private, urgent-to-fix, or both, and incorporated those into the vignettes. This follows our desire to learn *not* about devices

[1] This work is part of another study, but has been isolated to consider only the between-subjects aspects of the study. In the full study, participants were also asked a follow-up question about a smart light as a secondary device type (i.e., a within-subjects study).

specifically, but about the properties of those devices (privacy and urgency) in a more realistic setting.

The problem is that this approach still leaves room for participants to personally interpret a device's urgency or privacy. We felt it necessary, therefore, to be explicit about the device's privacy or urgency within our vignette (see Appendix A). We acknowledge that this solution is not perfect, but it gives us control over the scenario by having participants comment on a vignette presenting the privacy or urgency properties. To confirm the scenario with the way participants felt, we added questions on how the participants felt about the device's privacy and urgency. We took a closer look at this throughout Section 4.4.

3.2 Privacy threat model

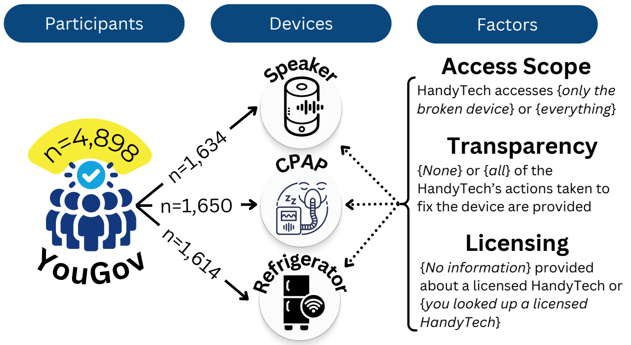
To better understand the privacy implications of fixing a smart home device with a HandyTech and the potential system-level interventions that exist, we first need to define our privacy threat model.

In the evolving ecosystem of smart home devices, it is possible to have a *centralized smart home system*, where a hub or an app can monitor and control all the smart home devices one owns. It means that there is a central hub or app that can monitor and control all the smart home devices one owns. We focus on centralized smart home systems because one of the major challenges of fixing smart home devices, as mentioned in Section 1, is that the dysfunction of a device may be caused by a different device due to the existence of home automation (e.g., trigger-action programs). If all smart home devices are managed separately, then the problem can be simplified to a usual electronic repair. In this paper, we seek to examine whetherpriva people are more or less willing to use a HandyTech who needs access to the entire network versus only a broken device.

The privacy risk that comes with a centralized system is that a HandyTech needs to be added to the system to view the status or the history logs of a smart home device. The challenge, however, is that many centralized smart home systems still use an all-or-nothing model for device-level access management [85]. We investigated major centralized smart home systems, including Google Home, Apple Home, Amazon Alexa, and Samsung SmartThings. As of the date of this study, only Samsung SmartThings supports device-level access control. Google, Apple, and Amazon do not have this type of granular, device-level control [7, 10, 34]. What this means for the latter three platforms is that an added user either has access to all devices or none—i.e., a HandyTech's access to one device means the HandyTech has access to all devices within the system.

3.3 Devices used in the study

CPAP is a form of therapy for managing health conditions such as obstructive sleep apnea or acute heart failure. Smart CPAP machines use heart rate or breathing patterns—likely sensitive information—to detect apneas and other irregularities during sleep, as well as the amount and quality of sleep. This information is stored and possibly transmitted to a physician or insurance company. In fact, insurance providers often require that CPAP data be transmitted to them in order to pay for the use of the CPAP machine. In turn, this makes the CPAP machine both a highly privacy-sensitive device and one that a participant might reasonably want to fix with great urgency.



Participants
Devices
Factors
n=4,898
YouGov
n=1,634
n=1,650
n=1,614
Speaker
CPAP
Refrigerator
Access Scope
HandyTech accesses {*only the broken device*} or {*everything*}
Transparency
{*None*} or {*all*} of the HandyTech's actions taken to fix the device are provided
Licensing
{*No information*} provided about a licensed HandyTech or {*you looked up a licensed HandyTech*}

Figure 1: Participants from YouGov randomly assigned one of three devices with per-factor random assignments. Factors are based on an all-or-nothing approach.

A smart refrigerator is a type of refrigerator that can connect to the Internet and perform a variety of automation tasks. These automation tasks can be simple, from tracking the stock of items on hand, to more complex, such as checking expiration dates on perishables. Given their connectivity, smart refrigerators can be controlled remotely using a smartphone or other smart device. Though debatable, the smart refrigerator was picked because it likely represents a lower privacy concern than other smart devices. While the items a person has in their fridge could arguably speak to socioeconomic status, advertiser-desired information for future conversions based on products purchased, and a variety of other types of privacy invasions [77, 78], prior work suggests that at least in terms of most or least privacy-invasive, the refrigerator is on the lower end of the spectrum [20, 57]. At the same time, the smart refrigerator is also highly urgent to fix, as most people do not want cooled items to go bad. This made the refrigerator a good option to assess high urgency and low(er) privacy.

The last device participants could have received was a smart speaker. The smart speaker is an Internet-enabled speaker that may be controlled by spoken commands (with the help of a "hot word") and is capable of streaming audio content, relaying information, and communicating with other devices. The canonical example of a smart speaker is Amazon's Alexa. This device was picked because it is likely on the low end of the spectrum for urgency to fix, and privacy-wise, this device is reasonably in the mid-to-high range. On the one hand, people do make sensitive voice commands to these devices, but on the other, the smart speaker may reasonably be viewed as less privacy-sensitive than an item like a CPAP or smart video camera. Given this mix, this device was picked because of its likely low urgency to fix and low-to-mid-range privacy concern.

In the next section, we describe the vignette, the measurement of variables, and our analysis methods in more detail.

3.4 Study design

We developed our survey by reviewing existing literature on vignette study design [46, 53, 56, 57], extensively discussing the survey with our research team, and making revisions and updates to the questions asked in an iterative fashion [71]. In the survey vignette, participants were told to imagine that the device they were randomly assigned was broken, but that a HandyTech (i.e., defined in the survey as someone who specializes in fixing smart home devices) could fix the device for them. Within each device condition, participants were given another series of randomized features about the HandyTech's work to evaluate how those are associated with willingness to use a HandyTech. We cover these in greater detail in Section 3.7.1, including the following conditions: access scope (i.e., less or more access to smart home data), licensing (i.e., whether HandyTech is licensed or not, implying some kind of certified training), and transparency (i.e., how aware could a customer be if they wanted to know what actions a HandyTech took in a repair). Figure 1 shows an overview of the procedure.

After learning about the device/condition and the HandyTech, participants were asked how willing they were to use a HandyTech to fix that device on a 5-point Likert scale (1=strongly disagree, 2=disagree, 3=neither agree nor disagree, 4=agree, 5=strongly agree). Specifically, participants responded to the statement: "I am willing to use this HandyTech to fix this device."

After the vignette, participants were asked additional survey questions. We sought to evaluate our priming about a device's urgency to fix and privacy sensitivity. After telling us if they were willing to use the HandyTech, participants were asked to respond to each of the following statements using the same 5-point Likert scale of strongly disagree to strongly agree: "I feel it is urgent to fix this device." And "I think that the data on this device is sensitive and private." We also included questions about the number and types of smart devices in their homes (i.e., would participants with more IoT devices be more willing to use a HandyTech?), and concerns about privacy related to smart devices. To evaluate participants' individual privacy concerns, we adapted three questions from prior surveys to specifically measure privacy concerns about smart devices rather than privacy concerns more generally or overall. First, we adapted two statements from the Deloitte 2023 Connected Consumer Survey about concerns that devices are vulnerable to security breaches, and that organizations or people could track them through their devices [14, 15]. We adapted the statements to use the term "think" instead of worry and specified "smart home devices" rather than simply "devices." The third privacy concern statement is adapted from the Pew Research Center's American Trends Panel, which asks people how concerned they are about how companies are using the data they collect [60]. We created a statement to gauge the extent of worry about how data gathered by smart home devices is used. We define our measures in more detail in Section 3.7.1. For the full survey instrument, see Appendix A.

3.5 Recruitment

Given that we sought participant opinions representative of the United States, we opted for a nationally represented survey that was distributed in collaboration with YouGov,[2] a market research platform that uses a proprietary double opt-in survey panel comprising approximately one million U.S. residents who have agreed to participate in YouGov's Web surveys. Our survey was piloted by YouGov, who also handled the dissemination of the survey. YouGov found that participants understood the questions and survey design. Participants are not paid to join the YouGov panel, but do receive incentives through a loyalty program to take individual surveys [97]. When joining the YouGov panel, panelists determine how often they receive survey invitations, with a maximum of one each day. The average number of completed surveys by a panelist in the last 30 days is two. The average tenure of YouGov panelists is 2.7 years. The average cooperation rate on YouGov is 21% (the cooperation rate is the "extent to which contacted individuals cooperate with a request to participate in a survey" [52]). The YouGov panel includes socio-demographic data on participant gender, age, race and ethnicity, education level, and family income.

Participants were matched by YouGov to a sampling frame on gender, age, race, and education. The sampling frame is a politically representative "modeled frame" of US adults, based upon the American Community Survey public use microdata file, public voter file records, the 2020 Current Population Survey Voting and Registration supplements, the 2020 National Election Pool exit poll, and the 2020 Current Employment Statistics surveys, including demographics and 2020 presidential vote. The matched cases were weighted to the sampling frame using propensity scores. The matched cases and the frame were combined, and a logistic regression was estimated for inclusion in the frame. The propensity score function included age, gender, race/ethnicity, years of education, region, and home ownership. The propensity scores were grouped into deciles of the estimated propensity score in the frame and post-stratified according to these deciles. The weights were then post-stratified on the 2020 presidential vote, as well as a four-way stratification of gender (binary), age, race, and education to produce the final population weight. We did not filter participants for required ownership or experience with smart home devices. We opted to include these participants because we felt that their perspective was valuable: We want to know how this percentage of the population feels about third-party IoT repair and the privacy concerns these repairs warrant. We also wanted our study to be representative, which would be skewed if we added filters like this.

3.6 Ethical considerations

The study was evaluated by the IRB at the University of Michigan and deemed to be exempt from review because the survey used a panel of participants, of which: (1) the identity of the human subjects could not readily be ascertained, directly or through identifiers linked to the subjects; and (2) any disclosure of the human subjects' responses outside the research would not reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, educational advancement, or reputation. As we commissioned YouGov for recruitment and survey distribution, YouGov handles the compensation through its own internal point systems, where the participants can earn points by completing surveys and redeeming points for various gift cards or cash. YouGov follows recommended best practice protocols for panel recruitment, informed consent per survey, and data quality [75, 94, 97]. We agreed with YouGov to follow all recommended practices as defined by human subjects research protocols. Only researchers listed on the IRB had access to survey data. When

[2] https://today.yougov.com/

accessing data, it was stored securely in a password-protected computer or in a secure third-party location, such as Google Drive.

3.7 Variable measurement

Our key research questions related to using a HandyTech are: who is willing? Do factors related to the work of the HandyTech influence their willingness? Does willingness to use one vary by how privacy-sensitive or urgent it is to fix the device? Our dependent variable is based on participants' responses to the statement "I am willing to use this HandyTech to fix this device" selecting one response from a 5-point Likert scale (strongly disagree to strongly agree). In our primary analyses, described in more detail in Section 3.8, we conduct linear regression to identify how individual characteristics, including concerns about smart home device privacy and security, as well as features of the HandyTech's work (access scope, licensing, transparency), and the types of devices (smart speaker, smart refrigerator, smart CPAP machine), are associated with willingness to use the HandyTech. We also examine how participants' assessments of a device's privacy and urgency-to-fix fit with our descriptions, and further use this variation to examine how device privacy and urgency are associated with willingness to use the HandyTech.

3.7.1 HandyTech work features.

In order to learn more about factors that may soon be recommended regarding technicians to install and repair smart home devices, we examine whether: (1) limiting access to the broken smart device, and/or (2) providing information that the technician is licensed, and/or (3) providing transparency about the repair work, increases willingness to use a third-party repair technician.

Access scope. When someone like a plumber comes to repair something like a broken bathroom sink, the customer is likely aware that the plumber will see and have access to everything in the bathroom where the sink is. It might even make sense for the plumber to see and have access to an adjacent room, if the plumbing is connected between the two. Given this knowledge, many people will tidy up a bathroom where the plumber is going to work, and may even tidy up nearby rooms if there is a chance the plumber will need to have such access. Likewise, some rooms may be considered off-limits to the plumber, such as the garage or a faraway bedroom. People may even lock certain doors that they do not want the plumber accessing. These actions are done in part to ensure that privacy is maintained when the third-party plumber makes a visit.

With this in mind, we follow our privacy threat model (Section 3.2) and provide a similar access-based system in the case of third-party IoT repair. It is easy to imagine that people would feel more comfortable with, and be more willing to use, a HandyTech who has limited access to potentially sensitive smart home data. However, given the potential cyber-physical interactions among the devices on the network, it is possible that the HandyTech may need to access the entire home network of all smart home devices in order to investigate the cause of the device not working. Therefore, to measure access scope, we use a randomized condition that states that the HandyTech requires either access to all devices on the home network or only the broken device. Although the access scope distinction could be finer-grained, we decided to focus on the experimentally testable extremes in this study, comparing access to either the broken device only or the entire network.

Licensing. State-based or federal licensing schemes seek to prevent harms that may occur in certain types of industries. For example, the likelihood of fraud by auto-mechanics—most people do not know how much certain auto parts should cost, have no way of verifying whether and how work was done, and a vehicle is a necessary tool for commuting to work—has led to the proliferation of state-based laws that mandate transparency about fees and the types of information that must be recorded about vehicle repairs [35]. Some industries also require a certain level of skill, or competency, to ensure safety, such as physicians. Finally, some industries mandate that workers carry insurance to ensure that errors or problems in providing a service may be amicably resolved. Licensing schemes bundle all of these policy interests together in order to cultivate a higher degree of trust in the use of a service. A "licensed" auto mechanic who may have a required amount of in-service skill training, for example, is likely more trustworthy and causes fewer safety errors than an unlicensed auto mechanic. Licensing does not comport with skill, but may serve as a proxy for trust and safety, potentially increasing willingness to use a service.

We measure the effect of licensing through a randomized condition that states either that the HandyTech is licensed or by having no statement about licensing in the vignette. We did not provide any specific details regarding who issues the license (e.g., government entity, industry body), what the licensing requirements are, or what aspects of the work are licensed. Instead, we sought to test simply whether describing the HandyTech as "licensed" or having no such description would influence willingness to use the HandyTech. If licensing matters, it may be important for future work to consider aspects of licensing specifically.

Transparency. Transparency is a common approach to building trust in services. In the auto-mechanic example listed above, transparency is often wrapped into consumer protection laws, given its efficacy in producing safer and more trustworthy services.

We measure transparency through a randomized condition that states either that the participant will or will not receive a list of all the HandyTech's actions to fix the device. We deliberately leave out details about how the list or log is designed, instead only telling participants that all the actions of the HandyTech will or will not be available. Our intention is not to determine how logs should be designed, but rather to test simply whether having transparency about the actions alone affects willingness to use a HandyTech. Future research is needed to better understand how the HandyTech's actions can be clearly and understandably presented to customers.

3.7.2 Individual characteristics.

We also sought to examine how individual concerns about smart home privacy may be related to willingness to use a HandyTech. As noted above, we adapted three statements about privacy from prior studies from Deloitte [14, 15] and Pew Research Center [60], using a 5-point Likert scale from strongly disagree (1) to strongly agree (5) as a response:

- I worry about how the data gathered by smart home devices could be used.
- I think that my smart home devices are vulnerable to security breaches.

- I think that organizations or people could track me through my smart home devices.

To measure smart home privacy concerns, we noted that the three variables were intercorrelated (r=.57-.59), with a Cronbach's alpha of 0.804. We computed a mean score by taking the average of the three variables. (Confirmatory factor analysis showed 1 factor explaining 72% of the variance. The factor score was correlated with our mean score at r=1.0, so we used the mean variable as a straightforward measure.)

In addition to individual privacy concerns about smart homes, we include individual demographic and household characteristics gathered as part of the panel survey. sThese include: binary gender (male/female), age, race/ethnicity, education level (college graduate/not a college graduate), family income, children (child < 18 years old live in home or not), marital status (married/partner versus not married), home type (single family versus other), homeowner (yes/no), number of smart home device types present in home (0-5+), region type (metropolitan/micropolitan/rural), and neighborhood owner-occupancy rate (based on zip code).

3.8 Analytic strategy

This section outlines our approach to analyzing our vignette study data to address our three research questions: who is willing to use a HandyTech (individual characteristics); which HandyTech factors (access scope, transparency, and licensing) affect willingness to use a HandyTech; and how the type of device, and perceptions of the device's urgency-to-fix or privacy sensitivity impact willingness.

Demographics and individual characteristics. First, we analyze the individual demographic and household characteristics associated with participants' willingness to use a HandyTech using multivariable OLS regression on the 5-point response to the statement "I am willing to use a HandyTech to fix this device."

HandyTech factors. We also use multivariable OLS regression to determine the effect of device types, and within each type of device, the effect of access scope, transparency, and licensing. Each model includes all individual demographic and household characteristics.

Urgency and privacy. Finally, we examine how participant perceptions of the levels of urgency and privacy for each device influence willingness to use the HandyTech. We utilize multivariable OLS regression for each separately, and then show how the interaction of perceived urgency and privacy affects willingness to use the HandyTech. Again, models include individual demographic, household, and vignette features.

In a series of sensitivity analyses, we consider the robustness of our findings in two different ways. First, we conduct our analyses on a subsample that includes only those participants who reported having one or more smart devices in the home. Our findings are substantively consistent with those reported below. Second, given that our dependent variable is an ordinal measure, we conduct alternative nonparametric analyses to evaluate the robustness of our findings. We tested ordinal regression models (both ordered logistic and ordered probit) of the Likert response on willingness to use HandyTech, but neither model met the proportional odds (i.e., parallel regression) assumption, indicating that the effects are not the same across all thresholds (cutpoints) of the ordinal outcome variable. Thus, we conducted a multi-variable binary logistic regression with the dependent variable as a dichotomous 0-1 variable (agree or strongly agree=1; neither agree nor disagree, disagree, strongly disagree=0) to analyze how our independent variables of interest affect the likelihood of agreeing to use the HandyTech or not. These findings are also substantively consistent with those reported below.

3.9 Limitations

Our study has a number of limitations that should be considered when interpreting the results. First, vignettes are artificial scenarios, which may not fully reflect the complexities and nuances of real-life situations, potentially limiting the generalizability of findings to real-world contexts [31]. Second, because vignettes present only a limited set of details by design, important contextual factors that could influence decision-making or perceptions may be omitted. A third limitation is that some vignette factors may be understood or interpreted differently across participants, which may introduce unexpected variance, limiting our ability to identify differences between our conditions. And although we attempted to make the survey less biased by limiting questions and attempting to present questions in a neutral way, traditional survey biases like fatigue, social desirability, and satisficing still apply [47, 48, 64].

Finally, our study represents the adult population of the United States only. We opted for the context of the United States as it was one we were familiar with. We do this in part because countries differ significantly in policies governing privacy as well as the use of new technologies, and so focusing on only one policy environment reduces the complexity of the model. It should not be assumed that the findings apply to settings outside the United States, and we urge future work to engage more deeply with these questions in other cultures and contexts.

We also would like to note that our survey aims to study *privacy* and *urgency-to-fix* in the setting of a HandyTech, instead of specific smart home devices. The specific devices were picked to highlight those properties (*privacy* versus *urgency-to-fix*). As noted in section 3.1, we primed participants of these properties in the vignettes. This deliberate study design is a common practice in simulating an environment for the purpose of a more precise study—as researchers often do in varying vignette conditions [3, 17, 84].

At the same time, this design in some ways primes participants to feel a certain way, which we acknowledge here as a limitation affecting our questions of willingness generally and, most particularly, Section 4.4. We use Section 4.4 to fully explore the variance in the way people felt about a device's urgency or privacy in order to evaluate the impact of our priming. We urge future work to look in more detail at how devices generally affect willingness without this type of explicit reference to privacy or urgency to fix.

4 Results

YouGov surveyed a nationally representative sample of 5,332 adults in the United States in 2024. The final sample of completed vignettes for this study is $n = 4,898$ participants. The total time to complete the survey was about 20 minutes. We next describe participant demographics and then provide results grouped around our three research questions.

Table 1: Participants

Gender (binary)		**Race/Ethnicity**	
Female	51%	Non-Hispanic white	63%
Male	49%	Hispanic	16%
		Non-Hispanic black	13%
Education		Asian/Asian American	4%
Not a college grad.	66%	Two+ races	2%
College grad.	34%	Other	2%
		Native American	1%
Age			
18–29	21%	**Children**	
30–39	16%	**No**	77%
40–49	15%	Yes	23%
50–59	16%		
60–69	19%	**Marital partner**	
70+	13%	No	51%
		Yes	49%
Annual family income			
Less than 30,000	24%	**Home type**	
30,000 - 49,999	15%	Single family	79%
50,000 - 99,999	29%	Multifamily	20%
100,000 - 149,999	14%	Other	1%
150,000 - 199,999	4%		
200K+	4%	**Homeowner**	
Prefer not to say	9%	Yes	67%
		No	33%
No. smart home devices			
5+	39%	**Neighborhood**	
2-4	34%	Metropolitan	85%
1	14%	Micropolitan	8%
None	13%	Rural	7%

4.1 Participant demographics

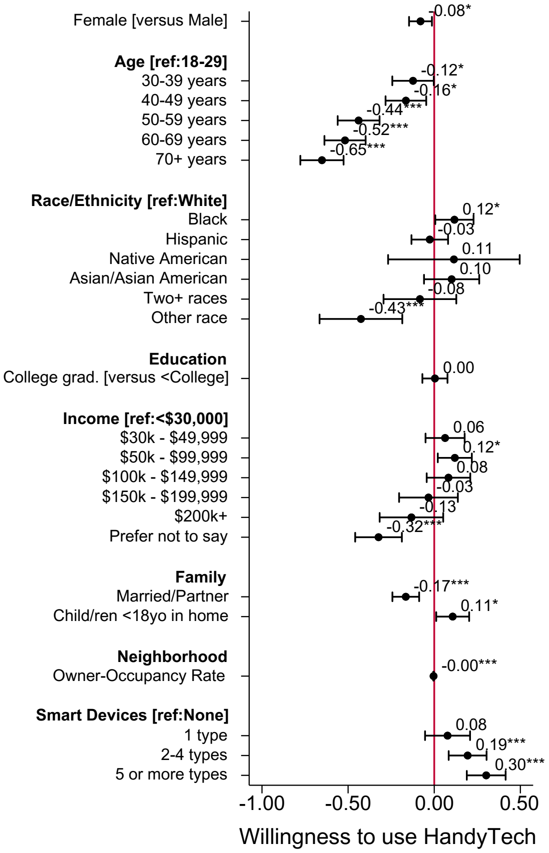
As this is a nationally representative sample of the United States, the participant demographics are similar to the population of the United States based on various sources detailed in Section 3.5.

More specifically, as shown in Table 1 (full details in Appendix B), 51% of participants are female, 63% report non-Hispanic white race, with 13% non-Hispanic black race, 16% Hispanic, 4% Asian/Asian American, 1% Native American, 2% reporting two or more races, and about 2% reporting another race. One-third of participants have a college degree or greater. About one-fifth of participants are between 18-29 years of age (21%), 31% are between 30 and 49 years, 26% are between 50 and 64 years, and 21% are aged 65 or more years. Over one-third of participants have annual incomes less than $50,000, while about one-fifth have annual incomes greater than $100,000. Nearly 10% of participants preferred not to report their income. We include these participants rather than dropping them because not sharing income information is a signal of privacy. Almost half of the participants report being married or living with a partner (49%) versus some other marital status, while about 23% report having at least one child under the age of 18 years old living in the home. Most participants live in a single-family dwelling (77%), and two-thirds own their homes. Only about 13% of participants said they had no smart devices in their homes, while the majority have two or more types of smart devices (73%).

4.2 Who is willing to use a HandyTech?

Figure 2 shows how individual characteristics affect willingness to use a HandyTech from the multivariable regression including all individual and vignette characteristics (full model results shown in the first column of Table 3 in the Appendix C). All else equal, women are less willing to use a HandyTech than men. Likewise, all adults 30 years or older are significantly less willing to use a HandyTech than those aged 18-29 years. There are no real differences in willingness by race and ethnicity, except that those who are included in the Other race category are less willing than those who are non-Hispanic White. There are no differences in willingness to use a HandyTech by education level.

Figure 2: Demographic impacts on willingness

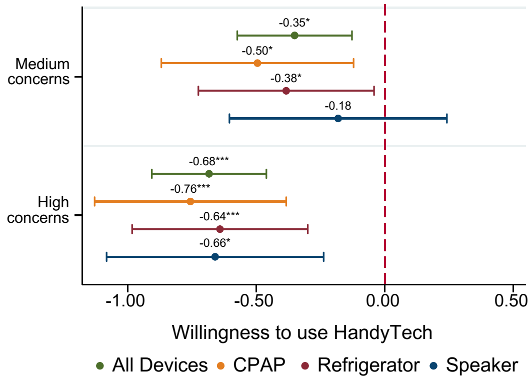


Who will use a HandyTech: OLS multi-variable regression coefficients for select individual, family, and neighborhood variables on willingness to use HandyTech, across all devices, controlling for all vignette characteristics and other non-significant variables (home ownership, household type including single-family and multiunit, and regional factors). Full model shown in Table 3 in the Appendix. *p < 0.05, **p < 0.01, ***p < 0.001

Family and household characteristics are also associated with willingness to use a HandyTech. Participants who are married or have a partner are less willing to use a HandyTech than those without a partner. It is unclear to us why marital status would be associated with willingness. In contrast, participants with one or more kids (under 18 years old) at home are more willing to use a HandyTech, though again it is unclear to us why these characteristics affect willingness.

Neither homeownership nor living in a single-family home significantly affects willingness to use a HandyTech, nor does geographic area (data not shown). The owner-occupancy rate of the neighborhood does, however, have higher rates associated with marginally but significantly less willingness. Ownership of smart

Figure 3: Privacy concern and willingness



OLS multi-variable regression coefficients for individual privacy concerns about smart devices on willingness to use HandyTech, across all devices and for each separate device (CPAP, Refrigerator, Speaker), controlling for vignette characteristics, sociodemographics, family characteristics, number of smart devices in home, and regional factors. *p < 0.05, **p < 0.01, ***p < 0.001

home devices, however, strongly influences the willingness to use a HandyTech. Those who own two or more types of smart devices are more willing to use a HandyTech compared to those who do not own any smart devices.

Figure 3 shows the impact of individual concerns about smart device privacy on willingness to use a HandyTech. Here we break out the effects for the model with all devices as well as for each type of device in the vignettes. Compared to those with low privacy concerns (the referent category), those with medium concerns are less willing to use a HandyTech overall and across each device, except for the smart speaker. Those with high concerns are less willing to use a HandyTech compared to those with low privacy concerns overall and for each device.

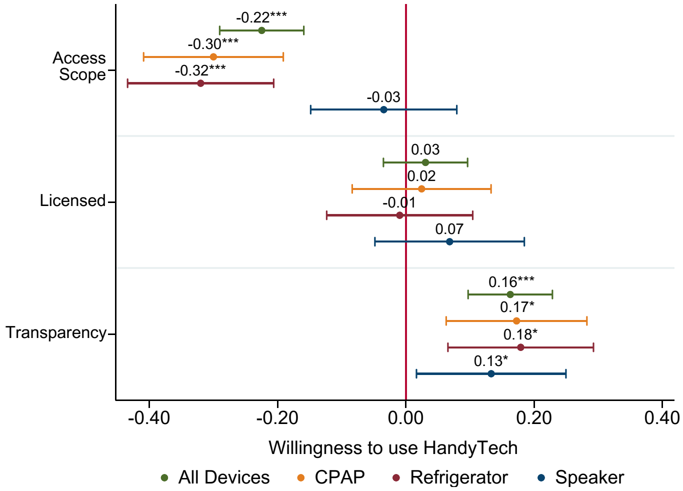
4.3 What factors (i.e., access scope, transparency, and licensing) influence the willingness of using a HandyTech?

We also sought to determine whether HandyTech work factors influenced willingness to use a HandyTech. As shown in Figure 4, both access scope and transparency affect willingness. On the contrary, the HandyTech being licensed had no statistically significant effect. The full model is displayed as Table 4 in Appendix C.

Willingness to use a HandyTech is lower when the HandyTech needs access to the entire home network (versus just the broken device) across all devices, and for the smart CPAP and smart refrigerator, but not the smart speaker. This finding indicates that the more access required by home IoT repair services, the less willing people are to use them.

Transparency about the HandyTech's actions taken to fix the device had the opposite effect, causing greater willingness to use a HandyTech for each and all devices. The finding indicates that smart device owners will want to have some information about the work the HandyTech has done in order to be willing to use them.

Figure 4: Factors impacting willingness



HandyTech work factors on willingness to use a HandyTech. OLS multi-variable regression coefficients for HandyTech work factors on willingness to use HandyTech across all devices and for each separate device (CPAP, Refrigerator, Speaker), controlling for sociodemographics, family characteristics, number of smart devices in home, privacy concerns, and regional factors. *p < 0.05, **p < 0.01, ***p < 0.001

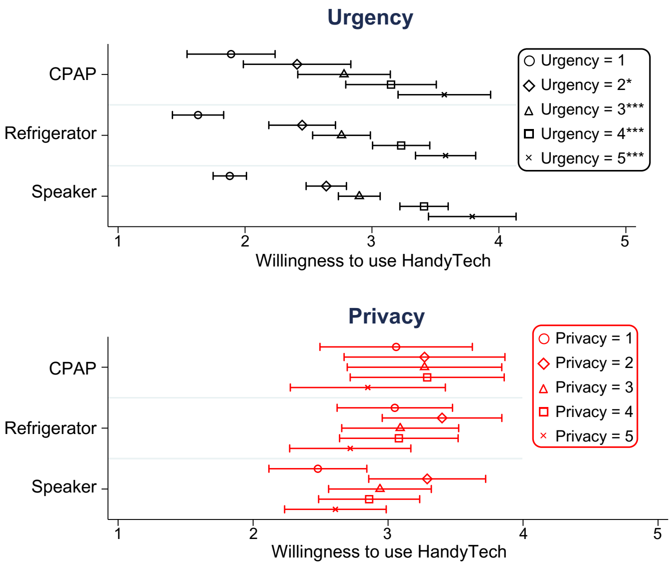
4.4 How does a device's privacy sensitivity and urgency-to-fix impact a participant's willingness to use a HandyTech?

We note that since we included statements about urgency and privacy with the type of device, we need to evaluate the impact of those statements on our results. As stated above, we based our vignettes around devices known to have those features. Here, we take a detailed look at how participants' perceptions of urgency and privacy sensitivity related to the device conditions affect the results for willingness to use a HandyTech.

The findings above about differences in the willingness to use a HandyTech between types of devices suggest that differences in device urgency and privacy may be influencing willingness to use a HandyTech. Because we hypothesized that the CPAP and refrigerator are more urgent to fix than the smart speaker, the CPAP and refrigerator conditions included the phrase "you want it to be fixed as soon as possible" whereas the smart speaker included the phrase "you don't think it is too urgent to fix." We tested the extent to which participants accepted these characterizations by asking them to respond to the statement "I feel it is urgent to fix this device." Participants agreed more strongly in both the CPAP and refrigerator conditions compared to the speaker condition: CPAP=3.9 > speaker=2.6, $F = 1273.2$, $p < .001$; refrigerator=3.7 > speaker=2.6, $F = 831.5$, $p < .001$ in contrast tests of marginal effects. There is no statistical difference in the perceived urgency to fix the device between the CPAP and refrigerator conditions.

Turning to privacy, recall that we hypothesized that the CPAP machine and the smart speaker are more privacy-sensitive than the refrigerator. For that, we primed the participants in the vignettes by saying that "you think that something more sensitive or private may get recorded" in the speaker condition, "you believe [it] includes

Figure 5: Per-Likert urgency and privacy



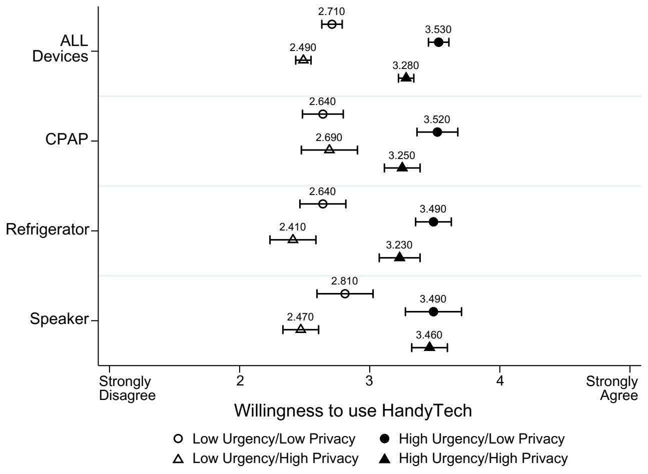
Showing the role of urgency and privacy on willingness to use a HandyTech for each device type. Average marginal effects of urgency to fix the device and privacy of data on the device in separate regressions of willingness to use a HandyTech (1=strongly disagree to 5=strongly agree) by device, controlling for sociodemographics, household characteristics, number of smart devices in the home, privacy concerns, and regional factors. *p < 0.05; **: p < 0.01; ***: p < 0.001.

sensitive, private information about you" in the CPAP condition, but "you don't think any sensitive or private information is collected by the device" in the refrigerator condition. We then tested the extent to which participants accepted these characterizations by asking them to respond to the statement "I think that the data on this device is sensitive, private information." Participants more strongly agreed with the statement in both the CPAP and speaker conditions, with both being statistically significantly higher than in the refrigerator condition: CPAP=3.93, speaker=3.98 > refrigerator=3.5, F = 188.7, p < .001 in contrast test of marginal effects.

Our findings that participants were more willing to use a HandyTech in the CPAP and the refrigerator conditions than in the speaker condition suggest that the urgency to fix the device may have a greater effect on willingness to use a HandyTech than the privacy sensitivity of the device. We thus run additional tests focusing on urgency and privacy. We tested these ideas by using the variation in participants' agreement with both device urgency and device privacy to examine their impact on willingness to use the HandyTech. That is, while we primed participants about these characteristics related to each type of device, there was still variation on both urgency and privacy agreement within each type of device. Indeed, for each type of device, participants gave responses from 1-5 to the statements about device urgency and privacy, so we used this variation to test the extent to which urgency and privacy perceptions influenced willingness to use the HandyTech for each device.

Figure 5 shows that willingness to use a HandyTech is associated with perceived urgency to fix the device within each type of device. That is, across each device, those who disagreed that it was urgent to fix the device (Urgency=1 or 2) were significantly less willing to use a HandyTech compared to those who agreed that it was urgent to fix the device (Urgency=4 or 5). In contrast, the same type of analysis applied to device privacy showed no significant effect on willingness to use a HandyTech for any of the devices. That is, variation in perceived privacy-sensitivity of the device did not affect willingness to use the HandyTech.

Figure 6: Willingness by low-high urgency and privacy

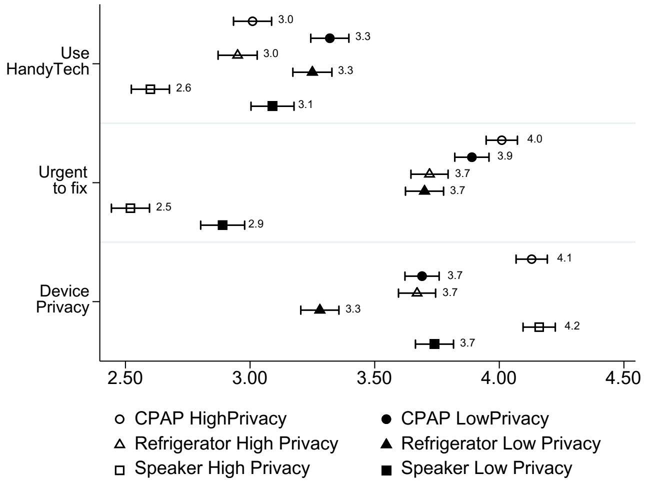


Showing willingness to use a HandyTech by perceptions of urgency and privacy of the device. Average marginal effects on willingness to use a HandyTech of the interaction of urgency to fix the device and privacy of data on the device in separate regressions by device, controlling for sociodemographics, household characteristics, number of smart devices in a home, privacy concerns, and regional factors.

Similarly, Figure 6 shows the results of an interaction between urgency and privacy on willingness. This analysis confirms the previous findings for urgency and privacy separately: for each type of device, those who perceived it was urgent to fix the device were more willing to use HandyTech regardless of the level of perceived privacy (i.e., HighUrgency/HighPrivacy and HighUrgency/LowPrivacy are always statistically significantly higher than either of the LowUrgency groups). However, two other interactions are also significant and suggest that device privacy interacts with urgency in ways that indicate privacy also matters—but that it varies between high and low urgency. For the CPAP condition, a high-urgency and high-privacy device, privacy tempered high urgency, such that those who perceived high urgency and high privacy were less willing to use HandyTech than those who perceived high urgency and low privacy (even though high privacy but low urgency was also lower). In contrast, for the low urgency and high privacy speaker condition, privacy tempered low urgency: those who perceived low urgency and high privacy were significantly less willing to use a HandyTech compared to those who perceived low urgency and low privacy. These findings indicate that urgency-to-fix a device strongly influences willingness to use a HandyTech, but that privacy also matters under some conditions—strong privacy concerns can dampen willingness for both high-urgency (e.g., CPAP machines) and low-urgency devices (e.g., speakers).

Finally, we tested how individual smart device privacy concerns (high versus low based on mean response to the three statements about smart home privacy, see Section 3.7.2) influence willingness

Figure 7: Individual privacy concerns



Showing individual privacy concerns about smart devices (high versus low). The first row contains scores for willingness to use a HandyTech. The second and the third show perceptions of urgency to fix the device and the privacy of the data on the device. Average marginal effects on willingness to use a HandyTech of the interaction of urgency to fix the device and privacy of data on the device in separate regressions by device, controlling for sociodemographics, household characteristics, number of smart devices in a home, privacy concerns, and regional factors.

to use a HandyTech, as well as how concerns are associated with perceptions of device urgency-to-fix and device privacy. As noted previously in Section 4.2 (Figure 3), those with high individual smart home privacy concerns are less willing to use a HandyTech. Figure 7 shows something similar—greater willingness to use HandyTech among those with low versus high privacy concerns for each type of device (top section in Figure 7).

Considering perceptions of urgency to fix the device, people with high privacy concerns agreed with a higher sense of urgency to fix the CPAP than those with low privacy concerns. In contrast, those in the speaker condition with high individual privacy concerns had a lower sense of urgency to fix the speaker. Individual privacy concerns made no difference in perceptions of urgency in the refrigerator condition. Considering perceptions of device privacy (bottom section in Figure 7, "Device Privacy"), those with high individual privacy concerns perceived device privacy to be higher across all devices.

In summary, greater perceived urgency to fix a device increases willingness to use a HandyTech. Perceived device privacy, however, seems to have a more nuanced effect. On the one hand, participants were very willing to use a HandyTech for the CPAP machine, even though it was perceived as a very privacy-sensitive device. But individual privacy concerns and device-privacy perceptions tempered their willingness, and across each device, individual privacy concerns lowered willingness to use a HandyTech.

5 Discussion

Our nationally representative study made several important findings. First, demographic and individual characteristics can greatly influence who is likely to use a HandyTech to fix a broken smart device. Those who own more types of smart devices and those who are younger in age are statistically significantly more likely to use a HandyTech. Likewise, while those who have greater privacy concerns are less likely to use a HandyTech for all devices except the refrigerator (where privacy concerns had no significant effect).

Second, factors like access scope and transparency influence people's willingness to use a HandyTech. Across all devices, the willingness to use a HandyTech is higher when the HandyTech has a more limited scope of access (i.e., accesses only the broken device). Similarly, transparency about the actions taken by HandyTech increases willingness to use a HandyTech. These findings are important not only because they are actionable to policymakers and developers, but also because they are likely to generalize to several other types of third-party repairs on privacy-sensitive devices. We view the HandyTech as a motivation for assessing issues where a repair person must access some sensitive data on a device in order to fix it. As such, these lessons may apply outside of the specific HandyTech context in which they are posed.

Third, perceived urgency to fix a device has a strong effect on the willingness to use a HandyTech. In our between-subjects analyses, we learned that although participants perceived a CPAP machine as highly private, they were nonetheless more willing to use a HandyTech to fix it compared to those with a broken smart speaker. Likewise, a high-urgency-to-fix device like a refrigerator also resulted in a higher willingness to use the HandyTech than the smart speaker. This finding, that urgency seemed to matter more than privacy, was actually more nuanced, with individual differences in privacy concerns and device privacy perceptions also influencing participants' hypothetical decision to fix or not fix a device with a HandyTech. We found that participants who had higher privacy concerns for devices were mostly less willing to fix those devices (see Figure 7). Likewise, participants who were more concerned with smart home privacy were mostly less willing overall to use the HandyTech (see Figure 3). These questions are further discussed under the umbrella of privacy as a calculus.

5.1 Privacy as a calculus

In Section 4.4, we found that both the perceived privacy and urgency of a device can affect one's willingness to use a HandyTech. The findings, in a way, reflect the concept of privacy calculus [51], which suggests that when making privacy-related decisions, people often weigh their perceived benefits (e.g., fixing devices when urgent) and their perceived costs (e.g., sharing data on the device). In the case of HandyTech, we found that when faced with urgent needs, people may be willing to use a HandyTech despite having privacy concerns. As a result, the urgency and necessity of getting the device fixed create an imbalanced power dynamic between customers and HandyTechs, forcing customers to share sensitive information, such as their medical data from the smart CPAP machine, to get their devices fixed promptly. Whether one's privacy might be violated or not solely depends on the integrity and trustworthiness of the HandyTech, which is not ideal.

Furthermore, our study also shows a significant interaction between perceived privacy and urgency. Interestingly, although privacy-conscious participants rated the smart CPAP machine as more private and more urgent to fix than the rest, their willingness to use a HandyTech was still significantly lower. On the other hand, for non-urgent devices like smart speakers, privacy-conscious participants also rate the urgency to fix the device significantly lower than the rest, which leads to the lowest willingness to use HandyTechs across all groups. Without properly addressing privacy concerns, third-party repairs on sensitive devices may create an extra barrier for privacy-conscious customers to receive the technical support they deserve, causing unfair treatment of customers.

Diluting the way someone feels about privacy and focusing on the utility that third-party repair services provide is not a great solution to this problem. A better solution may come from past studies in organization science. Here, researchers suggest that companies enforce procedural fairness, such as disclosing data practices (i.e., transparency) or providing more control to the customers, to increase the trust between companies and customers, which, in return, lowers customers' perceived cost of sharing their information [28]. Therefore, we believe procedural fairness, such as disclosing HandyTech's practices and enabling customers' control over the access, would be a positive avenue of development and regulation for industries, like the one we envision with the HandyTech, which rely on the repair of sensitive devices. Establishing such procedural fairness could be achieved through both technical design and policy enforcement. We detail our ideas in the following sections.

5.2 Recommendations for developers

5.2.1 Building transparency in smart home systems. Our study shows that the participants would be more comfortable with a HandyTech if they could be briefed about the actions that the HandyTech has taken to fix their devices (Section 4.3). It demonstrates the importance of having built-in transparency in smart home systems. Unfortunately, there are still challenges in understanding how to build transparency into smart home systems, and what should be included in the final report that can keep consumers effectively informed.

Transparency is a rising topic in the smart home domain, but most past studies focused on data practice transparency [43, 69] and network behavior transparency [67]. These studies provide valuable insights into manufacturers' data collection and usage, but neglect other potential stakeholders like the envisioned HandyTech in this paper. Most existing smart home systems provide some transparency on smart home devices' activities (e.g., "the lights turned on at 8 pm"). However, it is rare for these systems to record configuration changes, not to mention that the HandyTech may need access to lower-level features (e.g., error logs), disconnect and reconnect with the network, or even factory reset a device. Some repairs can also involve making physical changes to the device or interfering with the home network using external devices. Keeping the HandyTech accountable throughout these stages requires more work than recording device activities. Both technical solutions (e.g., recording low-level changes, tracing accessed data, and keeping the integrity of the records) and operational solutions (e.g., providing ethics training to certified HandyTech) should be simultaneously considered.

Another challenge is keeping consumers effectively informed about the repair work. Repairing a smart home device can involve many technical details. These details are often complicated and difficult to process. It is thus critical to understand what key information the consumers would like to see from a repair report, so that such information could be prioritized in the report. In addition, taking inspiration from the car repair industry, where a report is prepared when the job is done, we also believe some parts of the reports are not meant for consumers, but to hold the repair company accountable when a dispute occurs. Therefore, we suggest the report contain a summary of the repair, where the consumer can find the key information they would like to learn, and a fully detailed log of the actions that have been taken. Consumers should also be informed promptly of ways to resolve a dispute.

5.2.2 Varied access scope for repair. Our study provides some initial evidence that reduced access scope increases the participants' willingness to use a HandyTech. As discussed in Section 4.4, people do consider privacy, even though people often yield when the repair is urgent. People's desire for less access further enhances our argument that people would prefer a privacy-preserving option if such an option were available.

Providing minimal access would be ideal, but in the context of a HandyTech, what is considered "minimal" may be up for debate. Many smart home devices can be interconnected, either intentionally (e.g., home automation) or unintentionally (e.g., physical channels like temperature or lights [68]), making identifying the root cause of the failure more challenging. For example, a smart thermostat may automatically adjust temperatures based on residents' presence, provided by the smart lock. When the thermostat stops adjusting temperatures, it is easy to attribute the fault to the thermostat. However, it is also possible that the smart lock is faulty and sends the wrong information to the thermostat, causing the failure. In this case, the repair person must have access to both devices to determine the cause and resolve it. As a result, the desired access scope can be more complicated than the two options tested in our study.

We thus make a recommendation on the design of access grants for third-party IoT repairs. Granting access should be based on the relations between devices. The reason why the HandyTech may need access to multiple devices is that the failure on one device can be caused by another. Therefore, it is natural to think that the system could help the user to find all related devices in the first place, and grant HandyTech access to all the related devices upon approval. To find all potential devices, however, the system must consider both user-written automation and automation enabled through physical channels (e.g., turning on the oven can increase temperature, which triggers the AC to be turned on, even though the user has never written a rule to connect the two devices). Existing work has already explored ways to model possible interactions among smart home devices [68, 95]. How to leverage such techniques for an access control system is a question left for future work.

5.2.3 Iterative access granting through negotiation. It is fairly common for a traditional handyperson to request access to certain parts of the home, provided the handyperson explains, or it is known, why access is needed. Therefore, it could be natural for a third-party IoT repair person's initial access to be limited to the non-functioning device—it is assumed that this device needs to be accessed in order to be fixed. During the examination, however, if the repair person believes additional access is needed, a request could be made to the customer that specifies the request and provides an explanation. This, however, brings up a challenge. Unlike a traditional handyperson, who must be on-site, often accompanied by the consumer, an IoT repair person can conduct their work remotely, and the consumer may not be present to provide timely feedback. Similar to challenges in privacy negotiation among homeowners and guests [98], how the system could assist in reducing the communication overhead (e.g., automatically granting access if the device is not privacy-sensitive) can be another research direction to explore.

5.3 Recommendations for policymakers

Our findings highlight a power imbalance in the relationship between a technical IoT repair person and a consumer with a broken device. Imagine, for example, that a user feels it is urgent to fix their smart baby monitor because they feel a need to ensure that their infant is sleeping well at night. Further imagine that this video camera stores local footage from the past 48 hours and that the user knows it is likely that a repair person would be able to see all of that footage in the course of a repair. Parents are often highly privacy conscious and so the user may desire to limit access to the footage at all costs—but the device has to be fixed.

The user, just as in the case of a CPAP, is then likely to opt to have a HandyTech fix their device, even though a fix is to the detriment of their privacy. The real problem, however, is that the repair person is not necessarily incentivized to consider or accommodate those privacy concerns. The user is likely going to go forward with the repair anyway. Even if some of the technical measures discussed in Section 5.2 existed, the HandyTech may not have to follow those technical restrictions because the user wants the repair done. Additionally, similar to auto repairs, a user is unlikely to be able to watch or understand what exactly a repair person is doing, opening up avenues for abuse. Finally, smart home manufacturers, as overarching players in the IoT economy, may be indifferent, or even have opposite interests, when considering supporting this type of HandyTech industry. Better third-party repair means customers may be less likely to buy new products or pay for increased protection options often associated with new, rather than fixed, devices (e.g., Apple Care). Therefore, manufacturers may be disinclined to default to the type of privacy protections users desired in our study, namely, reduced access scope and increased transparency.

In turn, we make several recommendations for policymakers who could encourage or mandate that the IoT repair person industry follow best practices and balance out these relationships.

5.3.1 Policies for manufacturers. Policymakers should mandate smart home manufacturers (i.e., device manufacturers) to implement necessary access control and logging mechanisms to enable features like limited access and transparency. However, similar to regulations like the General Data Protection Regulation (GDPR) or the California Consumer Protection Act (CCPA), enforcing such requirements could take a long time and require years of multi-stakeholder effort. One potential solution, then, is to enforce such requirements only to smart home platforms (e.g., Google Home, Samsung SmartThings) instead of specific devices. Compared to the number of companies that produce smart home devices, the number of companies that develop smart home platforms is much lower. In addition, these new features could be released through software updates, instead of requiring consumers to buy new devices, reducing the potential friction during the process.

5.3.2 Policies for HandyTechs. From a policy-making perspective, it is hard to require a HandyTech to use limited access, as repairing smart home systems may require access to multiple devices or even the central system. What access is required must be evaluated on a case-by-case basis. However, transparency is much more straightforward to enforce. The HandyTech should provide customers with a list of actions they have taken on the smart home system and data they have viewed. It would be desirable that such logs are provided by the smart home system itself, so that there is no need for the HandyTech to acquire any extra devices for the logging process. Pushing this process onto the smart home itself also ensures the integrity of the log, as smart home systems do not have a vested interest in incorrect information. Of course, as mentioned in the previous paragraph, manufacturers must provide such functionalities to enable transparency, and a HandyTech would be unlikely to take this additional step without also being required to produce these logs.

In addition to limited access and transparency, we also think it is fruitful to further consider the possibility of enforcing licensing for the IoT repair industry. Although our study did not find that licensing had a significant effect on people's willingness to use a HandyTech, we believe it may have positive effects in protecting consumers' rights, and that the survey may not have shown this based on ambiguous understandings of what being a "licensed" HandyTech means. We opted for this design because we wanted to explore these topics in a nationally representative survey, and including all of the nuanced conditions we wished would have been difficult. Further studies, however, could further analyze licensing, exploring the ways a licensing scheme could neatly package many of our recommendations: (1) itemized receipts and actions taken in repair, which could be tied to a tiered type of access-based-transparency that presents a high-level perspective on how much of the home network the repair person pursued; and (2) requirements to carry insurance and have in-service training to ensure competency, encourage trust, and reduce abuse by adding friction to becoming an IoT repair person.

6 Conclusion

Smart devices are becoming increasingly prevalent in the home—a long-standing zenith of privacy protection [21, 27, 41, 76, 91]. These smart devices, interacting and storing some of the home's most intimate moments, will inevitably break. Looking to prior work, we investigate the role of a HandyTech, a skilled technician who is uniquely positioned to access and fix smart home devices, in turn also accessing the potentially sensitive data these devices contain [8]. We set out to understand how participants would perceive this privacy concern, using a series of vignettes with a nationally representative sample of adults in the United States: Who would use a HandyTech and why they would make that decision? We found that demographic groups, privacy-adjacent factors like scope of access, and a device's privacy sensitivity or urgency-to-fix are all relevant in a participant's determination to use a HandyTech.

Acknowledgments

This paper results from the SPLICE research program, supported by a collaborative award from the National Science Foundation (NSF) SaTC Frontiers program under award numbers 1955805, 1955172, 1955228, and 1955231. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of NSF. Any mention of specific companies or products does not imply any endorsement by the authors, by their employers, or by the NSF.

References

[1] Alessandro Acquisti, Curtis Taylor, and Liad Wagman. 2016. The economics of privacy. *Journal of Economic Literature* 54, 2 (2016), 442–492.

[2] Idris Adjerid, Eyal Peer, and Alessandro Acquisti. 2018. Beyond the Privacy Paradox. *MIS Quarterly* 42, 2 (2018), 465–488.

[3] Herman Aguinis and Kyle J. Bradley. 2014. Best practice recommendations for designing and implementing experimental vignette methodology studies. *Organizational Research Methods* 17, 4 (Oct. 2014), 351–371.

[4] 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.* 1–10.

[5] Hamoud Alhazmi, Ahmed Imran, and Mohammad Abu Alsheikh. 2022. How do socio-demographic patterns define digital privacy divide? *IEEE Access* 10 (2022), 11296–11307.

[6] Waqar Ali, Ghulam Dustgeer, Muhammad Awais, and Munam Ali Shah. 2017. IoT based smart home: Security challenges, security requirements and solutions. In *Proceedings of the 23rd International Conference on Automation and Computing.* 1–6.

[7] Amazon. 2025. How do household accounts work on Alexa devices? https://www.amazon.com/gp/help/customer/display.html?nodeId=GX3EC6SJYEPVNJKS [Accessed May 6, 2025].

[8] Denise Anthony, Carl A. Gunter, Weijia He, Mounib Khanafer, Susan Landau, Ravindra Mangar, and Nathan Reitinger. 2023. The HandyTech's coming between 1 and 4: Privacy opportunities and challenges for the IoT handyperson. In *Proceedings of the 22nd Workshop on Privacy in the Electronic Society.* 129–134.

[9] Ons Aouedi, Thai-Hoc Vu, Alessio Sacco, Dinh C Nguyen, Kandaraj Piamrat, Guido Marchetto, and Quoc-Viet Pham. 2024. A survey on intelligent internet of things: Applications, security, privacy, and future directions. *IEEE Communications Surveys & Tutorials* 27, 2 (2024), 1238–1292.

[10] Apple. 2025. Share control of your home. https://support.apple.com/en-us/102386 [Accessed May 6, 2025].

[11] Noah Apthorpe, Dillon Reisman, Srikanth Sundaresan, Arvind Narayanan, and Nick Feamster. 2017. Spying on the smart home: Privacy attacks and defenses on encrypted IoT traffic. *arXiv:1708.05044* (2017).

[12] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering smart home internet of things privacy norms using contextual integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 2 (July 2018), 1–23.

[13] Muhammad Aqeel, Fahad Ali, Muhammad Waseem Iqbal, Toqir A Rana, Muhammad Arif, and Md Rabiul Auwul. 2022. A review of security and privacy concerns in the internet of things (IoT). *Journal of Sensors* 2022, 1 (2022), 5724168.

[14] Jana Arbanas, Paul H. Silverglate, Susanne Hupfer, Jeff Loucks, Prashant Raman, and Michael Steinhart. 2023. Balancing act: Seeking just the right amount of digital for a happy, healthy connected life. https://www2.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey/2023/connectivity-mobile-trends-survey-full-report.html

[15] Jana Arbanas, Paul H. Silverglate, Susanne Hupfer, Jeff Loucks, Prashant Raman, and Michael Steinhart. 2023. Consumers embrace connected devices and virtual experiences for the long term. https://www2.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey/2023/connected-consumers-facing-new-reality-virtual-experiences.html

[16] Abeer Assiri and Haya Almagwashi. 2018. IoT security and privacy issues. In *Proceedings of the 1st International Conference on Computer Applications & Information Security.* 1–5.

[17] Christiane Atzmüller and Peter M. Steiner. 2010. Experimental vignette studies in survey research. *Methodology* 6, 3 (Jan. 2010), 128–138.

[18] Nazmiye Balta-Ozkan, Rosemary Davidson, Martha Bicket, and Lorraine Whitmarsh. 2013. Social barriers to the adoption of smart homes. *Energy Policy* 63 (Dec. 2013), 363–374.

[19] Birgul Basarir-Ozel, V. Aslihan Nasir, and Hande B. Turker. 2023. Determinants of smart home adoption and differences across technology readiness segments. *Technological Forecasting and Social Change* 197 (Dec. 2023), 122924.

[20] Chao Bian, Bing Ye, Anna Hoonakker, and Alex Mihailidis. 2021. Attitudes and perspectives of older adults on technologies for assessing frailty in home settings: A focus group study. *BMC geriatrics* 21, 1 (2021), 298.

[21] Dale Carpenter. 2012. *Flagrant conduct: The story of Lawrence v. Texas.* WW Norton & Company.

[22] Jason Ceci, Jonah Stegman, and Hassan Khan. 2023. No privacy in the electronics repair industry. In *Proceedings of the 2023 IEEE Symposium on Security and Privacy.* 3347–3364.

[23] Hossein Chegini, Ranesh Kumar Naha, Aniket Mahanti, and Parimala Thulasiraman. 2021. Process automation in an IoT–fog–cloud ecosystem: A survey and taxonomy. *IoT* 2, 1 (2021), 92–118.

[24] Sunil Cheruvu, Anil Kumar, Ned Smith, David M Wheeler, Sunil Cheruvu, Anil Kumar, Ned Smith, and David M Wheeler. 2020. IoT frameworks and complexity. *Demystifying Internet of Things Security* (2020), 23–148.

[25] Yong K Choi, Hilaire J. Thompson, and George Demiris. 2020. Use of an internet-of-things smart home system for healthy aging in older adults in residential settings: Pilot feasibility study. *JMIR Aging* 3, 2 (2020), e21964.

[26] Gordon Chu, Noah Apthorpe, and Nick Feamster. 2018. Security and privacy analyses of internet of things children's toys. *IEEE Internet of Things Journal* 6, 1 (2018), 978–985.

[27] Thomas P. Crocker. 2020. The Fourth Amendment at home. *Indiana Law Journal* 96 (2020), 167.

[28] Mary J. Culnan and Pamela K. Armstrong. 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science* 10, 1 (1999), 104–115.

[29] Tobias Dienlin, Philipp K. Masur, and Sabine Trepte. 2023. A longitudinal analysis of the privacy paradox. *New Media & Society* 25, 5 (2023), 1043–1064.

[30] Tobias Dienlin and Sabine Trepte. 2015. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology* 45, 3 (2015), 285–297.

[31] Fatemeh Erfanian, Robab Latifnejad Roudsari, Abbas Haidari, and Mohsen Noghani Dokht Bahmani. 2020. A narrative on the use of vignette: Its advantages and drawbacks. *Journal of Midwifery & Reproductive Health* 8, 2 (2020), 2134–2145.

[32] John J. Gallagher. 1970. Regulation of automotive repair services. *Cornell Law Review* 56 (1970), 1010–1030.

[33] Alexandar Joseph Gambino. 2023. Right to repair: Whose right is it anyway? *Transactions: Tenn. J. Bus. L.* 25 (2023), 125.

[34] Google. 2025. Manage people and permissions in the Google Home app. https://support.google.com/googlenest/answer/15681236 [Accessed May 6, 2025].

[35] Neil Gunningham. 2002. Regulating small and medium sized enterprises. *Journal of Environmental Law* 14 (2002), 3.

[36] S. M. Taiabul Haque, MD Romael Haque, Swapnil Nandy, Priyank Chandra, Mahdi Nasrullah Al-Ameen, Shion Guha, and Syed Ishtiaque Ahmed. 2020. Privacy vulnerabilities in public digital service centers in Dhaka, Bangladesh. In *Proceedings of the 2020 International Conference on Information and Communication Technologies and Development.* 1–12.

[37] Weijia He, Jesse Martinez, Roshni Padhi, Lefan Zhang, and Blase Ur. 2019. When smart devices are stupid: Negative experiences using home smart devices. In *Proceedings of the 2019 IEEE Security and Privacy Workshops.* 150–155.

[38] Weijia He, Nathan Reitinger, Atheer Almogbil, Yi-Shyuan Chiang, Timothy J. Pierson, and David Kotz. 2024. Contextualizing interpersonal data sharing in smart homes. *Proceedings on Privacy Enhancing Technologies* 2024, 2 (2024), 295–312.

[39] Christian Pieter Hoffmann, Christoph Lutz, and Giulia Ranzini. 2016. Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10, 4 (2016).

[40] Christine Horne, Brice Darras, Elyse Bean, Anurag Srivastava, and Scott Frickel. 2015. Privacy, technology, and norms: The case of smart meters. *Social Science Research* 51 (2015), 64–76.

[41] Josh Howarth. 2024. 50+ smart home statistics (new 2024 data). https://explodingtopics.com/blog/smart-home-stats#

[42] James Imgraben, Alewyn Engelbrecht, and Kim-Kwang Raymond Choo. 2014. Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour & Information Technology* 33, 12 (2014), 1347–1360.

[43] Haojian Jin, Gram Liu, David Hwang, Swarun Kumar, Yuvraj Agarwal, and Jason I. Hong. 2022. Peekaboo: A hub-based approach to enable transparency in data processing within smart homes. In *Proceedings of the 2022 IEEE Symposium on Security and Privacy.* 303–320.

[44] Tae Hee Jo, Jae Hoon Ma, and Seung Hyun Cha. 2021. Elderly perception on the internet of things-based integrated smart-home system. *Sensors* 21, 4 (Jan. 2021), 1284.

[45] Jana Juric and Jörg Lindenmeier. 2019. An empirical analysis of consumer resistance to smart-lighting products. *Lighting Research & Technology* 51, 4 (2019), 489–512.

[46] Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security* 64 (2017), 122–134.

[47] Jon A. Krosnick, Sowmya Narayan, and Wendy R. Smith. 1996. Satisficing in surveys: Initial evidence. *New directions for evaluation* 1996, 70 (1996), 29–44.

[48] Ivar Krumpal. 2013. Determinants of social desirability bias in sensitive surveys: a literature review. *Quality & Quantity* 47, 4 (2013), 2025–2047.

[49] Deepak Kumar, Kelly Shen, Benton Case, Deepali Garg, Galina Alperovich, Dmitry Kuznetsov, Rajarshi Gupta, and Zakir Durumeric. 2019. All things considered: An analysis of IoT devices on home networks. In *Proceedings of the 28th USENIX Security Symposium*. 1169–1185.

[50] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, are you listening?: Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (Nov. 2018), 1–31.

[51] Robert S. Laufer and Maxine Wolfe. 1977. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues* 33, 3 (1977), 22–42.

[52] Paul J. Lavrakas. 2008. *Encyclopedia of survey research methods*. Sage publications.

[53] Haein Lee, Hyejin Park, and Jinwoo Kim. 2013. Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies* 71, 9 (2013), 862–877.

[54] Li Li, Tianfeng Li, Hua Cai, Jian Zhang, and Jianjun Wang. 2023. I will only know after using it: The repeat purchasers of smart home appliances and the privacy paradox problem. *Computers & Security* 128 (2023), 103156.

[55] Zied Mani and Inès Chouk. 2017. Drivers of consumers' resistance to smart products. *Journal of Marketing Management* 33, 1-2 (2017), 76–97.

[56] Davit Marikyan, Savvas Papagiannidis, and Eleftherios Alamanos. 2019. A systematic review of the smart home literature: A user perspective. *Technological Forecasting and Social Change* 138 (Jan. 2019), 139–154.

[57] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020. "You just can't know about everything": Privacy perceptions of smart home visitors. In *Proceedings of the 19th International Conference on Mobile and Ubiquitous Multimedia*. 83–95.

[58] Kirsten Martin and Helen Nissenbaum. 2016. Measuring privacy: An empirical test using context to expose confounding variables. *Columbia Science and Technology Law Review* 18 (2016), 176–218.

[59] M. Hammad Mazhar and Zubair Shafiq. 2020. Characterizing smart home IoT traffic in the wild. In *Proceedings of 2020 IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation*. 203–215.

[60] Colleen McClain, Michelle Faverio, Monica Anderson, and Eugenie Park. 2023. How Americans view data privacy. https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

[61] Faith McCreary, Alexandra Zafiroglu, and Heather Patterson. 2016. The contextual complexity of privacy in smart homes and smart buildings. In *HCI in Business, Government, and Organizations: Information Systems*. 67–78.

[62] Phoebe Moh, Pubali Datta, Noel Warford, Adam Bates, Nathan Malkin, and Michelle L. Mazurek. 2023. Characterizing everyday misuse of smart home devices. In *Proceedings of the 2023 IEEE Symposium on Security and Privacy*. 2835–2849.

[63] Nur Mohammad, Rabeya Khatoon, Sadia Islam Nilima, Jahanara Akter, MD Kamruzzaman, and Hasan Mahmud Sozib. 2024. Ensuring security and privacy in the internet of things: challenges and solutions. *Journal of Computer and Communications* 12, 8 (2024), 257–277.

[64] Jonathan Mummolo and Erik Peterson. 2019. Demand effects in survey experiments: An empirical assessment. *American Political Science Review* 113, 2 (2019), 517–529.

[65] Pardis E Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Cranor, and Norman Sadeh. 2017. Privacy expectations and preferences in an IoT world. In *Proceedings of the Thirteenth Symposium on Usable Privacy and Security*. 399–412.

[66] Helen Nissenbaum. 2009. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press. 304 pages.

[67] TJ OConnor, Reham Mohamed, Markus Miettinen, William Enck, Bradley Reaves, and Ahmad-Reza Sadeghi. 2019. HomeSnitch: Behavior transparency and control for smart home IoT devices. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. 128–138.

[68] Muslum Ozgur Ozmen, Xuansong Li, Andrew Chu, Z. Berkay Celik, Bardh Hoxha, and Xiangyu Zhang. 2022. Discovering IoT physical channel vulnerabilities. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*. 2415–2428.

[69] Sunyup Park, Anna Lenhart, Michael Zimmer, and Jessica Vitak. 2023. "Nobody's happy": Design insights from privacy-conscious smart home power users on enhancing data transparency, visibility, and control. In *Proceedings of the Nineteenth Symposium on Usable Privacy and Security*. 543–558.

[70] D. Pavithra and Ranjith Balakrishnan. 2015. IoT based monitoring and control system for home automation. In *Proceedings of the 2015 Global Conference on Communication Technologies*. 169–173.

[71] Verónica Pérez Bentancur and Lucía Tiscornia. 2024. Iteration in mixed-methods research designs combining experiments and fieldwork. *Sociological Methods & Research* 53, 2 (2024), 729–759.

[72] Jason Pridmore, Jessica Vitak, Daniel Trottier, Yuting Liao, Michael Zimmer, Anouk Mols, and Priya C. Kumar. 2019. Intelligent personal assistants and the intercultural negotiations of dataveillance in platformed households. *Surveillance and Society* 17, 1-2 (2019), 125–131.

[73] Julie Ramhold. 2023. Can you still buy a non-smart TV. https://www.dealnews.com/features/tv/smart-tv/

[74] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2017. Where is the digital divide? A survey of security, privacy, and socioeconomics. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 931–936.

[75] Federal Regulations. 2009. Protection of human subjects. *National Institutes of Health Office for Protection from Research Risks* 45 (2009).

[76] Nathan Reitinger and Amol Deshpande. 2023. Epsilon-differential privacy, and a two-step test for quantifying reidentification risk. *Jurimetrics: The Journal of Law, Science & Technology* 63, 3 (2023), 263–317.

[77] Nathan Reitinger, Bruce Wen, Michelle L. Mazurek, and Blase Ur. 2023. Analysis of Google ads settings over time: Updated, individualized, accurate, and filtered. In *Proceedings of the 22nd Workshop on Privacy in the Electronic Society*. 167–172.

[78] Nathan Reitinger, Bruce Wen, Michelle L. Mazurek, and Blase Ur. 2024. What does it mean to be creepy? Responses to visualizations of personal browsing activity, online tracking, and targeted ads. *Proceedings on Privacy Enhancing Technologies* 2024, 3 (2024), 715–743.

[79] Faisal Saeed, Anand Paul, Abdul Rehman, Won Hwa Hong, and Hyuncheol Seo. 2018. IoT-based intelligent modeling of smart home environment for fire prevention and safety. *Journal of Sensor and Actuator Networks* 7, 1 (2018), 11.

[80] Neelima Sailaja, Teresa Castle-Green, Paul Coulton, Michael Stead, Joseph Lindley, Lachlan Urquhart, and Dimitrios Paris Darzentas. 2023. UbiFix: Tackling repairability challenges in smart devices. In *Adjunct Proceedings of the 2023 ACM International Joint Conference on Pervasive and Ubiquitous Computing & the 2023 ACM International Symposium on Wearable Computing*. 802–806.

[81] S. Sujin Issac Samuel. 2016. A review of connectivity challenges in IoT-smart home. In *Proceedings of the 3rd MEC International Conference on Big Data and Smart City*. 1–4.

[82] Frederik Schuster and Abdolrasoul Habibipour. 2024. Users' privacy and security concerns that affect IoT adoption in the home domain. *International Journal of Human-Computer Interaction* 40, 7 (April 2024), 1632–1643.

[83] Wentao Shang, Yingdi Yu, Ralph Droms, and Lixia Zhang. 2016. *Challenges in IoT Networking via TCP/IP Architecture*. Technical Report NDN-0038. Named Data Networking.

[84] Jessica Sheringham, Isla Kuhn, and Jenni Burt. 2021. The use of experimental vignette studies to identify drivers of variations in the delivery of health care: A scoping review. *BMC Medical Research Methodology* 21, 1 (April 2021), 81.

[85] Amit Kumar Sikder, Leonardo Babun, Z. Berkay Celik, Hidayet Aksu, Patrick McDaniel, Engin Kirda, and A. Selcuk Uluagac. 2022. Who's controlling my device? Multi-user multi-device-aware access control system for shared smart home environment. *ACM Transactions on Internet of Things* 3, 4 (Sept. 2022), 27:1–27:39.

[86] Vijay Sivaraman, Hassan Habibi Gharakheili, Arun Vishwanath, Roksana Boreli, and Olivier Mehani. 2015. Network-level security and privacy control for smart-home IoT devices. In *Proceedings of the 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications*. 163–167.

[87] Sean Smith. 2017. *The Internet of risky things: Trusting the devices that surround us*. O'Reilly Media, Inc.

[88] Daniel J. Solove. 2006. A taxonomy of privacy. *University of Pennsylvania Law Review* 154, 3 (2006), 477.

[89] Daniel J. Solove. 2021. The myth of the privacy paradox. *George Washington Law Review* 89 (2021), 1.

[90] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, and Rahul Chatterjee. 2023. "It's the equivalent of feeling like you're in "jail"': Lessons from firsthand and secondhand accounts of IoT-enabled intimate partner abuse. In *Proceedings of the 32nd USENIX Security Symposium*. 105–122.

[91] William J. Stuntz. 1998. Distribution of Fourth Amendment privacy. *George Washington Law Review* 67 (1998), 1265.

[92] Panjun Sun, Shigen Shen, Yi Wan, Zongda Wu, Zhaoxi Fang, and Xiao-zhi Gao. 2024. A survey of IoT privacy security: Architecture, technology, challenges, and trends. *IEEE Internet of Things Journal* (2024).

[93] Lo'ai Tawalbeh, Fadi Muheidat, Mais Tawalbeh, and Muhannad Quwaider. 2020. IoT privacy and security: Challenges and solutions. *Applied Sciences* 10, 12 (2020), 4102.

[94] Joe Twyman. 2008. Getting it right: YouGov and online survey research in Britain. *Journal of Elections, Public Opinion and Parties* 18, 4 (2008), 343–354.

[95] Qi Wang, Pubali Datta, Wei Yang, Si Liu, Adam Bates, and Carl A. Gunter. 2019. Charting the Attack Surface of Trigger-Action IoT Platforms. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 1439–1453.

[96] Meredydd Williams, Jason RC Nurse, and Sadie Creese. 2016. The perfect storm: The privacy paradox and the internet-of-things. In *Proceedings of the 11th International Conference on Availability, Reliability and Security*. 644–652.

[97] YouGov. 2025. Methodology. https://today.yougov.com/about/panel-methodology [Accessed May 3, 2025].

[98] Haozhe Zhou, Mayank Goel, and Yuvraj Agarwal. 2024. Bring privacy to the table: Interactive negotiation for privacy settings of shared sensing devices. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*.

A Survey Instrument

A.1 Definitions

[DEFINITIONS to be shown at beginning of survey, and available (via embedded popup) when the <term> is used.]

Throughout the survey, the following terms are used:

Smart home device: A smart home device is an internet network-connected device (connected via Wi-Fi, Bluetooth, or similar protocols) that is used to remotely control functions or physical aspects of the home. Smart devices can include appliances, thermostats, lights, and other devices, including personal and wearable health devices. Smart systems in homes can be set up through wireless or hardwired systems.

Smart home device app: A smart home device app is an application on your smartphone, computer, laptop, or tablet that is used to remotely control or access your smart home device.

CPAP machine: Continuous positive airway pressure (CPAP) is a form of therapy for managing health conditions such as obstructive sleep apnea or acute heart failure. CPAP therapy uses machines specifically designed to deliver a flow of air at a constant pressure through a hose connected to a mask or tube worn by the patient (often at night to treat obstructive sleep apnea).

Smart CPAP machine: Smart CPAP machines use your heart rate or breathing patterns to detect apneas and other irregularities in your sleep and record the amount of sleep you get and the quality of your sleep. Smart CPAP machines can store and transmit data and measurements about how often you use it, as well as about your sleep, and the device effectiveness. Insurance providers often require that data be transmitted to them in order to pay for the use of the CPAP machine. Your doctor may also receive the data to monitor your treatment.

Smart light: Smart lights are lighting fixtures and light bulbs that can sense and interact automatically with their environments, other smart devices, and with users. Depending on the type, users can control smart bulbs with a remote control, or from an app on your phone, or by giving voice commands via a digital voice assistant or smart display.

Smart speaker: an internet-enabled speaker that is controlled by spoken commands (with the help of a "hot word") and is capable of streaming audio content, relaying information, and communicating with other devices. The built-in microphone in smart speakers is continuously listening for "hot words" followed by a command, [but it is not always clear what is being recorded, how recorded data will be used, or how it will be protected.]

Smart system: A smart system in a home allows users to control certain "smart" devices remotely using a smartphone or tablet through an internet connection. Smart devices can include appliances, thermostats, lights, and other devices, including personal and wearable health devices. Smart systems in homes can be set up through wireless or hardwired systems.

Data/Information broker: A data broker, sometimes called an information broker, is a business that collects personal data from various sources, processes it, and sells it to individuals or companies for marketing, risk mitigation, and other purposes, such as data to screen potential tenants for landlords and real estate companies.

The **privacy** of smart home devices refers to the right of a party to maintain control over and be assured confidentiality of personal information that is collected, transmitted, used, and stored during the use of smart home devices.

The **security** of smart home devices refers to the prevention of damage to, unauthorized use of, and exploitation of smart home devices and the information they contain, in order to strengthen the confidentiality, integrity, and availability of these devices. In this survey, "security" is equivalent to "cybersecurity." Physical security related to the home or its occupants is different and will be referred to as "home security."

[vignette conditions: First randomization]
[1. Device type: A=smart speaker/voice assistant; B=refrigerator; C=CPAP machine] randomized

Imagine you have **[A | B | C]**

A (a <smart speaker> like Amazon Alexa or Google Home, with a voice assistant built-in. You can ask it questions or give it commands and it will provide responses to you. The speaker records your past conversations with it and listens for your commands. Although you generally ask it common questions, you do think that something more sensitive or private may get recorded. One day, you notice the smart speaker is not working. Since your daily routines do not rely on the speaker, you don't it is too urgent to fix, but you would like it fixed anyway.)

B (a <smart refrigerator> which has an online interface that can show you recipes and track your shopping list. Because you picked a version that does not contain any cameras or microphones, you don't think any sensitive or private information is collected by the device. One day, you notice the smart refrigerator is not working. Worrying the food inside could spoil, you want it to be fixed as soon as possible.)

C (a <smart CPAP machine> that helps you breathe properly during your sleep. Due to your physical condition, you use it every night. The machine records your sleep time and some medical information about your sleep, which you believe includes sensitive, private information about you. One day, you notice the CPAP machine is not working. Since you rely on it to help you sleep in a healthy way, you want it to be fixed as soon as possible.)

You recently heard about something called a HandyTech - someone who specializes in fixing smart home devices. Once hired, this person can inspect your smart home device remotely and then fix any smart home devices that are not working.

[vignette conditions: second randomization]
[2. License A=no license; B=license]

A (You looked up a HandyTech available in your local town. You contact the HandyTech to fix [the device].)

B (You looked up a HandyTech available in your local town, and find one who is licensed. You contact the HandyTech to fix [the device].)

The HandyTech said that you won't be charged if the device is not fixed. Before you pay, you will be able to check if the device is fixed by turning it on and off to see if it has been fixed.

[3. Transparency A= no info on actions; B= info on actions/log]

A You can observe whether the HandyTech has fixed the device or not, but not any of the specific actions taken by the HandyTech. You agree that the amount to be charged to fix [the device] is fair and acceptable to you.

B The HandyTech also told you that once the job is done, you will receive a list of all the actions taken to fix the device. You agree that the amount to be charged to fix [the device] is fair and acceptable to you.)

[4. Access scope A=access data from only affected device; B= Access data from any smart home drive on the home network]

A The HandyTech tells you they will need access to data recorded by [the device] only. No data from any other smart home devices on your home network would be accessed to identify the problem and fix the device.

B The HandyTech tells you they will need access to data recorded by [the device] and any other smart home devices on your home network to identify the problem and fix the device.

[Survey Questions – asked after the vignette]
Having now read about the HandyTech in this scenario, how much do you agree or disagree with the following statements: [same response items for each question]

1. I am willing to use this HandyTech to fix this device.
2. I feel it is urgent to fix this device.
3. I think that the data on this device is sensitive, private information.

RESPONSE OPTIONS:

- Strongly disagree
- Disagree
- Neither agree nor disagree
- Agree
- Strongly agree

A.2 Next are some questions about your use of smart devices

Which of the following <smart home devices> do you have in your home? RESPONSE OPTIONS

(1) no
(2) yes
(3) not sure

(Select all that apply.):

- Virtual voice assistants and smart speakers (e.g., Amazon Echo/Alexa, Google Nest Home Hub, Apple HomePod)
- Thermostats (e.g., Nest, Ecobee)
- Video doorbell (e.g., Ring Video doorbell)
- Home security devices (e.g., cameras, door locks, garage door openers)
- Smart Lighting (e.g., lightbulbs, lighting systems)
- Home environment sensors (e.g., smoke and leak detectors)
- Appliances (e.g., refrigerators, washing machines/dryers, ovens, coffee makers/espresso machines)
- Entertainment (e.g., TVs, streaming devices such as AppleTV or Roku)
- Plugs or outlets (e.g., Wemo Mini, Wyze Plug)
- Domestic robots that do household chores (e.g., robot vacuums such as iRobot Roomba, smart lawn mowers)
- Smart health devices (e.g., wearable fitness device like Fitbit, internet-connected Glucose monitor or blood pressure monitor or CPAP machine)
- Smart home hubs (e.g., Samsung SmartThings, Hubitat Elevation, AppleHomeKit) *Does not include voice assistants/smart speakers like Google Nest Hub or Amazon Echo. Those would be considered virtual voice assistants/smart speakers (#1)
- Other (e.g., smart windows solutions, smart watering system, smart pet feeder) (please specify):

A.3 How much do you agree or disagree with the following statements about smart home devices: [Randomized grid]

RESPONSE OPTIONS:

(1) Strongly disagree
(2) Disagree
(3) Neither agree nor disagree
(4) Agree
(5) Strongly agree

- I worry about how the data gathered by smart home devices could be used.
- I think that my smart home devices are vulnerable to security breaches.
- I think that organizations or people could track me through my smart home devices.

B Full Demographics Table

Table 2: Participants

Characteristics	Unweighted	Weighted		
	N	%	95% CI	
Binary Gender				
Male	2304	48.6	47.2	50.1
Female	2594	51.4	49.9	52.8
Race/Ethnicity				
Asian/Asian American	179	3.7	3.1	4.3
Hispanic	704	15.9	14.8	17.2
Native American	50	1.0	0.8	1.4
Non-Hispanic Black	606	12.5	11.5	13.6
Non-Hispanic White	3145	62.9	61.4	64.3
Two+ Races	121	2.3	1.9	2.8
Other	93	1.7	1.3	2.0
Education				
Not a College Graduate	3180	66.3	64.9	67.7
College Graduate	1718	33.7	32.3	35.1
Age				
18−29 years	836	20.9	19.7	22.3
30−39 years	783	16.4	15.3	17.6
40−49 years	781	15.1	14.1	16.2
50−59 years	849	15.7	14.7	16.7
60−69 years	965	18.5	17.4	19.7
70+ years	684	13.3	12.4	14.3
Annual Family Income				
Less than $30,000	1166	23.9	22.6	25.2
30, 000−49,999	747	15.3	14.2	16.4
50, 000−99,999	1435	29.1	27.8	30.5
100, 000−149,999	668	13.6	12.7	14.7
150, 000−199,999	220	4.4	3.8	5.0
$200,000 or more	206	4.3	3.7	4.9
Prefer not to say	456	9.4	8.5	10.3
Children				
Does Not Have Children	3804	77.3	76.1	78.6
Has Children	1094	22.7	21.4	23.9
Marital Partner				
Married	2449	48.6	47.1	50.1
Unmarried	2449	51.4	49.9	52.9
Home Type				
Single Family Home	3758	79.1	77.8	80.3
Multifamily	983	20.0	18.8	21.2
Other	46	0.9	0.7	1.2
Homeowner				
Non-Owner	1710	33.4	32	34.8
Owner	3188	66.6	65.2	68
Number of Smart Home Device Types				
None	659	13.2	12.3	14.3
1	679	13.7	12.7	14.7
2-4	1678	34.3	32.9	35.7
5+	1882	38.8	37.4	40.3
Neighborhood Type				
Metropolitan	4155	85	84	86.1
Micropolitan	408	8.3	7.5	9.1
Rural	335	6.7	6	7.5

C Additional Tables

Table 3: Average marginal effects of Individual Characteristics on Willingness to Use a HandyTech, across all and for each smart device, weighted OLS regression models.

Individual Characteristics	ALL Devices			Smart CPAP			Smart Refrigerator			Smart Speaker		
	AME	CI		AME	CI		AME	CI		AME	CI	
		Lower	Upper		Lower	Upper		Lower	Upper		Lower	Upper
Gender (ref: Male)												
Female	-0.08*	-0.15	-0.01	-0.14*	-0.25	-0.03	-0.03	-0.14	0.09	-0.06	-0.18	0.06
Age (ref: 18–29 years)												
30–39 years	-0.12*	-0.24	-0.002	-0.19*	-0.38	-0.002	-0.11	-0.32	0.11	-0.08	-0.30	0.14
40–49 years	-0.16**	-0.28	-0.05	-0.24*	-0.44	-0.05	-0.13	-0.34	0.07	-0.15	-0.36	0.06
50–59 years	-0.44***	-0.56	-0.32	-0.47***	-0.66	-0.27	-0.40***	-0.61	-0.18	-0.46***	-0.67	-0.25
60–69 years	-0.52***	-0.64	-0.40	-0.61***	-0.81	-0.42	-0.50***	-0.70	-0.30	-0.46***	-0.68	-0.25
70 years or older	-0.65***	-0.78	-0.53	-0.68***	-0.89	-0.46	-0.75***	-0.97	-0.53	-0.54***	-0.76	-0.33
Education (ref: less than college)												
College Degree	0.004	-0.07	0.08	0.07	-0.06	0.19	0.01	-0.04	0.07	-0.01	-0.14	0.11
Race/ethnicity (ref: non-Hispanic White)												
Hispanic	-0.03	-0.13	0.08	-0.02	-0.18	0.15	-0.12	-0.31	0.32	0.05	-0.14	0.25
Native American	0.11	-0.27	0.50	-0.0002	-0.51	0.51	0.26	-0.44	0.96	0.06	-0.49	0.60
Non-Hispanic Asian	0.10	-0.06	0.26	0.10	-0.16	0.37	0.18	-0.12	0.48	-0.21	-0.29	0.25
Non-Hispanic Black	0.12*	0.01	0.23	0.17	-0.01	0.36	0.15	-0.03	0.33	0.03	-0.16	0.24
Non-Hispanic Other race	-0.43***	-0.67	-0.19	-0.63**	-1.01	-0.25	-0.39	-0.80	0.02	-0.29	-0.78	0.20
Two+ Races	-0.08	-0.29	0.13	-0.27	-0.64	0.09	0.09	-0.23	0.42	-0.09	-0.47	0.30
Marriage (ref: not married)												
Married/Partner	-0.17***	-0.24	-0.09	-0.08	-0.21	0.05	-0.14*	-0.27	-0.01	-0.26***	-0.40	-0.12
Child/Children under 18 in home (ref: none)												
Have child/children under 18	0.11*	0.01	0.20	0.15*	0.0003	0.31	0.002	-0.17	0.17	0.16	-0.01	0.33
Homeowner (ref: renter)												
Other	0.03	-0.06	0.12	0.16*	0.01	0.31	-0.10	-0.25	0.05	0.04	-0.13	0.20
Annual Income (ref: <$30,000)												
$30-49,999	0.06	-0.05	0.18	0.09	-0.09	0.28	0.17	-0.02	0.36	-0.08	-0.29	0.12
$50-99,999	0.12*	0.02	0.22	0.09	-0.07	0.25	0.31***	0.14	0.47	-0.03	-0.21	0.15
$100-149,999	0.08	-0.04	0.21	-0.04	-0.25	0.17	0.30***	0.09	0.52	-0.01	-0.24	0.21
$150-199,999	-0.03	-0.20	0.14	-0.19	-0.49	0.10	0.07	-0.24	0.38	0.03	-0.25	0.30
$200,000 or more	-0.13	-0.32	0.05	-0.21	-0.55	0.13	0.03	-0.30	0.36	-0.22	-0.51	0.07
Prefer not to say	-0.32***	-0.46	-0.19	-0.29*	-0.52	-0.06	-0.24*	-0.48	-0.001	-0.41**	-0.65	-0.17
Home Type (ref: single-family)												
Multi-unit	-0.03	-0.06	0.12	0.22**	0.07	0.37	-0.13	-0.29	0.04	-0.19*	-0.37	-0.01
Smart Devices in Home (ref: none)												
1 Type	0.08	-0.05	0.21	-0.05	-0.27	0.18	0.24*	0.01	0.46	0.04	-0.19	0.26
2-4 Types	0.19**	0.08	0.30	0.04	-0.14	0.23	0.31**	0.12	0.49	0.26**	0.06	0.46
5 or more Types	0.30***	0.19	0.41	0.15	-0.04	0.34	0.40***	0.21	0.60	0.33***	0.13	0.53
Privacy concerns about smart homes	-0.28***	-0.32	-0.23	-0.22***	-0.29	-0.15	-0.28***	-0.36	-0.21	-0.32***	-0.41	-0.24
Neighborhood Owner-occupancy rate	-0.003***	-0.006	-0.002	-0.002	-0.005	0.001	-0.003	-0.01	0.001	-0.01***	-0.01	-.003
Location (ref: metropolitan)												
Micropolitan	0.02	-0.11	0.14	-0.04	-0.24	0.16	0.06	-0.15	0.28	-0.01	-0.24	0.23
Rural	-0.001	-0.15	0.15	-0.20	-0.48	0.07	0.17	-0.06	0.40	-0.05	-0.30	0.22
R^2	0.179			0.168			0.187			0.188		
N	4,692			1,578			1,554			1,560		

Source: Author-designed vignette study with YouGov representative panel survey.

Note: AME=average marginal effect; CI=confidence interval; Ref: referent category.

All models include variables controlling for the vignette conditions.

*: p < 0.05; **: p < 0.01; ***: p < 0.001

Table 4: Coefficients of Vignette factors (types of devices, and HandyTech work features) on Willingness to Use a HandyTech, across all and for each smart device, weighted OLS regression models.

Vignette Characteristics	ALL Devices			Smart CPAP			Smart Refrigerator			Smart Speaker		
	AME	CI		AME	CI		AME	CI		AME	CI	
		Lower	Upper		Lower	Upper		Lower	Upper		Lower	Upper
Vignette Device Type (ref: smart speaker)												
Smart Refrigerator	0.27***	0.19	0.35	—			—			—		
Smart CPAP	0.34***	0.26	0.42	—			—			—		
Licensing (ref: not licensed)												
Licensed	0.03	-0.03	0.10	0.03	-0.08	0.13	-0.01	-0.12	0.10	0.07	-0.05	0.18
Transparency (ref: none provided)												
Provided	0.16***	0.10	0.23	0.17**	0.06	0.28	0.18**	0.07	0.29	0.13*	0.02	0.25
Access (ref: limited access)												
Full access	-0.23***	-0.29	-0.16	-0.30***	-0.41	-0.19	-0.32***	-0.43	-0.21	-0.03	-0.15	0.08

Source: Author-designed vignette study with YouGov representative panel survey.

Note: AME=average marginal effect; CI=confidence interval; Ref: referent category.

All models include variables controlling for individual and household characteristics.

*: p < 0.05; **: p < 0.01; ***: p < 0.001