The HandyTech's Coming Between 1 and 4: Privacy Opportunities and Challenges for the IoT Handyperson

Denise Anthony
deniseum@umich.edu
University of Michigan

Carl A. Gunter
cgunter@illinois.edu
University of Illinois at Urbana-Champaign

Weijia He
weijia.he@dartmouth.edu
Dartmouth College

Mounib Khanafer*
mkhanafer@auk.edu.kw
American University of Kuwait

Susan Landau
susan.landau@tufts.edu
Tufts University

Ravindra Mangar
ravi.gr@dartmouth.edu
Dartmouth College

Nathan Reitinger
nlr@umd.edu
University of Maryland

ABSTRACT

Smart homes are gaining popularity due to their convenience and efficiency, both of which come at the expense of increased complexity of Internet of Things (IoT) devices. Due to the number and heterogeneity of IoT devices, technologically inexperienced or time-burdened residents are unlikely to manage the setup and maintenance of IoT apps and devices. We highlight the need for a "HandyTech": a technically skilled contractor who can set up, repair, debug, monitor, and troubleshoot home IoT systems. In this paper, we consider the potential privacy challenges posed by the HandyTech, who has the ability to access IoT devices and private data. We do so in the context of single and multi-user smart homes, including rental units, condominiums, and temporary guests or workers. We examine the privacy harms that can arise when a HandyTech has legitimate access to information, but uses it in unintended ways. By providing insights for the development of privacy control policies and measures in-home IoT environments in the presence of the HandyTech, we capture the privacy concerns raised by other visitors to the home, including temporary residents, part-time workers, etc. This helps lay a foundation for the broad set of privacy concerns raised by home IoT systems.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**.

KEYWORDS

IoT, home IoT, privacy harms, IoT handyperson

*Corresponding author

WPES '23, November 26, 2023, Copenhagen, Denmark

ACM ISBN 979-8-4007-0235-8/23/11.
https://doi.org/10.1145/3603216.3624956

ACM Reference Format:
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 21st Workshop on Privacy in the Electronic Society (WPES '23), November 26, 2023, Copenhagen, Denmark.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3603216.3624956

1 INTRODUCTION

Smart homes offer convenience: the ability to turn up the heating before you arrive home or to remotely monitor that the burglar alarm is working. But that convenience comes at the cost of complexity. Typically, a smart home is an environment with multiple users with different interests, levels of technological awareness and capabilities, and perceptions of authority and privileges. Who should have permission to control smart home appliances? What authority do different family members or occupants get? What about guests or temporary workers in a home? Do landlords have full control over smart home devices in accommodations they lease?

The complexity extends in another direction too. How do we handle the interoperability of different home Internet of Things (IoT) systems? What happens when there are unexpected interactions between the various cyber-physical systems of home IoT devices? In an industrial setting such as a manufacturing plant, this complexity would be handled by a company systems administrator. The smart home equivalent would be a "HandyTech": a contractor who can set up and remove home IoT systems and monitor, maintain, and debug them as they are used.

This situation raises many sociological, legal, and technical questions. Who gets to control the smart home devices? The residents of the dwelling? The owner? Or the building manager of an apartment building or residential housing community? We focus here on the privacy risks raised by a HandyTech hired to manage the technology. What are their responsibilities with respect to residents' privacy? How can this be achieved?

Because of the potential for complex interactions between smart home devices, such a HandyTech will need access to relevant devices. Thus the HandyTech is an individual who, in the absence of access control policies, has the ability to gain full access to the IoT

platform in a smart home and retrieve private data that may reveal the daily routines of the home's occupants.

Smart home IoT deployments involve not simply the reality of turning up the air conditioner while driving home or lying in bed and being able to shut off the downstairs lights by saying so, but the reality of multiple people, with different roles, seeking to manage the systems: house occupants, landlord, condo manager, and house guest or worker.

As a result of potential interaction of the cyber-physical systems that home IoT devices operate, for a HandyTech to successfully manage home IoT deployments, they must have access to home IoT devices and also to logs of previous actions. That is, the HandyTech will necessarily have access to recent information about the use of home IoT devices. This is a superset of the information sought by any manager of a home IoT system, whether the housing manager of an apartment or condo complex, a landlord, or a head of household. In understanding the privacy issues raised by HandyTech access, we illuminate the privacy issues of all managers of home IoT systems—and thus our paper speaks to more than just the HandyTech situation.

Given that our work is examining a profession that does not yet exist, at least in the manner we are describing, we note our assumptions. Because the concept of a HandyTech is new, a "HandyTech" does not yet have a definitive job description. We imagine this individual to be a technologically savvy contractor who helps home residents, house managers, landlords, and others, with home IoT problems. But this is an assumption, not reality, and this assumption impacts the opportunities and challenges we discuss.

With this assumption in mind, we note that the closest literature here concerns the smart home as a *multi-user* environment. Researchers have largely focused on the privacy harms from a guest [19] visitor [15], incidental user [12], or bystander [28] may encounter when visiting a smart home. Some work focused on the privacy risks associated with monitoring or tracking visitors by home IoT devices [2, 6, 26]. Other studies focused on granting visitors owner-like privileges [3, 4, 23, 24]. Privacy notices and their usefulness in raising privacy awareness among home users and bystanders have been studied in [25]. There has, however, been related work that occurs in a somewhat different venue: smartphone repair shops [1, 10]. None of this work involves access of the type assumed by a HandyTech.

As noted above, privacy issues in smart homes are broader than that relatively narrow focus. They also involve what the managers of the smart home systems can access about home residents and short-term and long-term visitors and workers in the home. By focusing on the presence of a *skillful technician* whose job is to *access* the IoT platform and conduct diagnostic and troubleshooting tasks, we look at a superset of privacy issues faced by residents and visitors—and thus illuminate these issues.

In this paper, we explore the complexity of a smart home and introduce the concept of a HandyTech, noting benefits of a HandyTech and identifying key privacy challenges this role raises. We use the Citron and Solove descriptions of privacy harms [11] to delineate possible privacy harms stemming from a HandyTech's actions (or inactions) and suggest various approaches (technical, legal, and policy) to protect against these harms.

2 MOTIVATION

To motivate the concept of a HandyTech, we contrast the deployment and operation of security systems in homes in the early 2000s to IoT deployments today (e.g., Control4 [13]). Around the year 2000, companies like ADT Security Systems typically provided installation in homes of equipment such as keypads and alarms. These were then connected to a monitoring service using protocols like DUAL-Tone Multi-Frequency (DTMF). The monitoring systems were commonly staffed by a collection of agents, working directly for the providing vendor or outsourced.

If the system issued an alert, the agents would carry out a sequence of steps such as asking for a PIN, sounding an alarm, or calling the police. Such human agents reduced potential false negatives (e.g., an alarm accidentally set by the homeowner) and enabled custom assistance to homeowners during stressful events.

By contrast, today's security services are commonly based on IoT and have many more features supporting security and convenience. Wireless protocols and low-energy sensors make it possible for the consumer to procure and deploy devices throughout the house at their discretion, eliminating the cost and inconvenience of hiring workmen to install wires around the house. IoT-based solutions also offer a form of self-monitoring that enables a homeowner to perform many of the functions a monitoring agent might have performed: an alert on the homeowner's smartphone suffices in many cases. This can be enhanced by location monitoring so the alarm system is likely to know if the homeowner is present. Increasingly advanced capabilities such as the use of facial recognition and advanced sensor capabilities offer even more functionality. However, these capabilities can increase complexity and risk.

While these advances provide many benefits, the systems may create unmanageable complexities. Stories about opaque configuration and malfunctions of IoT devices that give rise to situations like home owners who cannot turn off their IoT lights are common. In general, there is an explosion of new functions and new ways to combine them. HandyTech aims to improve this complex and risky state of affairs by the integration of a form of "human-in-the-loop."

A HandyTech for IoT provides the potential for benefits—but there are also potential drawbacks. For instance, there are security risks that arise from increasing the attack surface for the IoT system by including more parties with permissions. A professional HandyTech who knows when to apply an essential update may be using access control wisely. A homeowner who puts their tech-savvy teenager in charge of the updates may have a different outcome. While security is a key concern, it may be that the bigger challenge concerns privacy. To be useful, the HandyTech needs to have some knowledge of the homeowner systems. How to specify what the homeowner considers private and what information should be accessible to for the HandyTech may not be an easy call.

3 HANDYTECH: CONCEPT AND BENEFITS

As IoT devices propagate into our domestic spaces, the role of the HandyTech—a skilled technician capable of navigating the complexities of home IoT systems—emerges as crucial.

Concept. The HandyTech is responsible for setting up, maintaining, and troubleshooting IoT systems, including everything from routers and firewalls to smart appliances. The HandyTech also serves as

the "human-in-loop," helping homeowners manage the intricate balance between functionality, privacy, and security.

A HandyTech's role is diverse and requires a broad skill set. They need to be well-versed in the protocols and standards across different IoT vendors to ensure system interoperability. Their expertise extends beyond just hardware repair to diagnosing network issues, making them uniquely equipped to handle the layered complexities introduced by IoT devices. The HandyTech's role may not include *all* repairs of malfunctioning home IoT devices, but cover software, firmware, and networking functions. A failed discharge pump in a dishwasher or a broken compressor in an air-conditioning unit will need a dishwasher or air conditioner repairman, not the HandyTech (though the HandyTech may be able to diagnose the problem). As devices get smarter and capable of self-diagnosis, the HandyTech role is expected to evolve rather than be replaced, especially as they consult with homeowners on trade-offs between competing system needs like security versus ease-of-use.

HandyTech access to in-home data itself raises significant privacy concerns. In addition, the HandyTech must be diligent in restricting access to logs as well as the IoT data gathered by the smart device and in educating homeowners about potential security vulnerabilities. While automated diagnosis tools and AI systems like ChatGPT may make strides in simplifying the interface between homeowners and their smart systems, the HandyTech remains an invaluable human intermediary for making informed choices in complex home IoT ecosystems.

Benefits. Deploying and maintaining smart home devices can be overwhelming and challenging [18], but a HandyTech can provide great benefits to users. Similar to how some smart home devices require professional installation (e.g., smart thermostats may require writing an HVAC system to a smart home product), HandyTech can simplify and enable such installation while ensuring safety and code compliance. Even if a smart home device is easy to install, set up and deployment may be challenging. For example, the precise placement of motion sensors is crucial for automation. Installation might be frustrating if sensors are hard to detach and reattach [27]. The complexity could also arise when a smart home device is integrated with other smart home devices or ecosystems. A smart lightbulb can be controlled by its own app, a smart hub (e.g., Philips Hue), or a voice assistant. Maintenance and commission thus become tedious and confusing. Here is where experience counts. A HandyTech possesses the expertise to install complex smart systems efficiently.

The complexity of smart home devices may confound residents when devices break. When a non-smart light fails, residents know to check the bulb, fixture, outlet, or electric panel. However, smart home system failures can originate from issues beyond those, such as a faulty companion app, a network outage, or an unresponsive motion sensor that activates the lightbulb. A HandyTech, unlike homeowners, has the expertise to identify the source of the problem.

Many smart home device complaints are about security [14]. Setting up network-level smart home security and privacy technologies [16, 17, 22] is typically difficult for the average user to do. Discovering and recovering a compromised smart home device is also difficult for such users. Even if a user can identify a compromised device and fix it, the user may fail to prevent a repeat compromise due to leaving the vulnerability unpatched (e.g., weak authentication) that enabled the attack in the first place. A HandyTech's expertise in security products and standards of care can greatly aid in mitigating such security risks. The HandyTech could protect a smart home by setting up proper firewalls or a guest network. Similarly, a HandyTech could use intrusion-detection tools and know the proper hosts and ports to find devices with unusual behaviors [20]. Indeed, a vendor-certified HandyTech would possess expertise that regular users would be unlikely to have.

Another potential benefit of the HandyTech would be their ability to assist residents with customizing the system to their privacy preferences (e.g., preventing data collection at night). Such assistance would be valuable for home residents and would require a HandyTech to have a thorough grasp of potential privacy issues of IoT devices and systems.

In short, a HandyTech can provide a variety of security, safety, privacy, and simplifying benefits to smart home residents.

4 PRIVACY IMPLICATIONS

Home is where a person most expects to be unobserved. Such privacy is not always achievable; in a shared living space, for example, an individual's privacy might only be had in a bedroom or bathroom—or when no one else is present at home. In group arrangements, such as college dormitories, residents may not always feel they have full privacy even within their home. Nonetheless, in all cultures, home is considered a private space.

Enabling the HandyTech to diagnose malfunctions within home IoT systems requires providing them with access to a significant range of Home IoT devices and network logs. Such access intrudes on a resident's privacy—and may occur without residents' knowledge (e.g., by a HandyTech accessing home IoT information remotely). Laws and policy currently have little to say on this issue. Before such regulation can occur, however, a more fundamental issue is the nature of privacy harms that could result from HandyTech access to home IoT records. That is the question we examine here.

Following [7], we say that the use of data constitutes a privacy failure if an "entity" has legitimate access to information, but uses the data in ways unintended by the user. We use characterizations of privacy harms developed by Citron and Solove [11] to briefly discuss the types of privacy harms that may occur if a HandyTech were to inappropriately use information obtained about home IoT.
Physical harms. As the HandyTech is in a position to control the home IoT devices, they could set devices to work in ways that could cause damage.

Economic harms. Some actions that the HandyTech takes—or does not take—can be privacy violations. Patterns of residents' daily lives and knowledge of account information (e.g., Netflix, Amazon, Internet providers) are easily discernible from data of home IoT devices [5, 21]; sharing such information could lead to robbery and identity theft.

Reputational harms. Few people behave in exemplary ways all the time; home is a location in which people let down their guard. A HandyTech is in a position to cause reputational harm should they inappropriately share the information about behavior inside the home.

Psychological harms. Knowledge of what happens inside the home—the all-seeing eye that the HandyTech can develop —means that they can attain the understanding of home behavior and dynamics more akin to someone living in the home. Even if never acted upon, that fact can cause distress to home occupants and residents. Such psychological concerns (and thus such harms) are likely felt differently by different social groups, e.g., stigmatized groups, women compared to men.

Autonomy harms. The HandyTech's access to intimate aspects of a person's life could lead to user's self-constraining use of systems. While data about individual smart home devices is likely to often be available at equipment manufacturers, more complete data will be accessible by the HandyTech. The fact that such data are increasingly used by law enforcement can lead to "system avoidance": people systematically avoid institutions that keep formal records, including hospital, banks, schools, and employment [8, 9].

Discrimination harms. As noted in (5), the knowledge that the HandyTech gains about activities within the home can be used for various forms of control of the residents.

Relationship harms. Because private aspects of home life may now be exposed (e.g., how much time particular people spend together) to a third party inherently destroys some intimacy in relationships.

This brief discussion suggests that privacy risks from HandyTech have significant dependence on the types of workflows of which they are a part. In Appendix A, we present a short case study for a realty scenario that illustrates this point.

5 FUTURE DIRECTIONS

The idea of pursuing a business model in which sales are encouraged by access to knowledgeable experts is common. Apple helps consumers understand their Apple products by talking to an Apple "Genius," while Best Buy aids deployments of products it sells with help from the "Geek Squad." But in a world in which products can interact, expertise is needed beyond that provided by a single manufacturer or sales outlet. In this paper, we have proposed an innovative—and, we suspect, necessary—way to handle this issue: the complexity arising from smart home IoT from the residents' point of view. We also discussed privacy issues that might arise from our proposed solution, the HandyTech. In the process, we have uncovered more questions than answers.

In answering these questions, we urge others to study various dimensions of the HandyTech role. Scenarios such as the one in the appendix Appendix A present the complexities arising in the sale of a smart home and the role that a HandyTech would play in ensuring a transfer that protects the buyer's and seller's privacy Studying such examples will illuminate the complexity of privacy concerns within smart homes with more than a single resident.

Regardless of which form a HandyTech-type solution takes, the role is not only achievable, but necessary. Thus, one aspect of future research will be to understand industry's solutions for tackling the dual problems of smart home complexity and inherent conflicts between different residents' needs. That will enable a more nuanced solution for capabilities that a HandyTech should have and the controls that should govern such access.

Another aspect may be to understand how current efforts in smart home platforms, like Matter, will support the HandyTech role. As Matter's main target is to achieve secure device interoperability, the protocol's specifications cover access control and privileges of home IoT administrators. However, understanding how the HandyTech's role should be accommodated and what privileges or restrictions should be placed on the role will be instrumental in how a HandyTech operates.

Finally, it is inevitable that a HandyTech will require access to data of home IoT devices, but what level of access is reasonable? For example, when the lighting is malfunctioning, granting a HandyTech access to a smart thermostat may not make sense, but if the thermostat affects lighting automation, it might be reasonable. As with other questions raised by a HandyTech, this issue extends well beyond the role.

6 CONCLUSIONS

In this paper we have shed light on the concept of a HandyTech, a skilled technician who helps smart home users set up, troubleshoot, and maintain their home IoT system. Given the increasing complexity and popularity of smart homes, the HandyTech's role—or something like it—is likely to be essential in the coming years. We have explored the qualifications necessary for the role, highlighted the benefits and challenges this role brings, and explored the privacy implications of such a role. Much remains to be done.

Do we expect a HandyTech to work exactly as we have posited? Absolutely not! But do we expect that if home IoT takes off in the way that industry and the government expect, there will be a societal need for some version of the HandyTech we have described? Without question, there will be. So what we have sought to do here is describe the type of role the HandyTech will fulfill, delineate in some detail the resulting privacy threats the role of the HandyTech will create, and propose solutions, some technical and some policy/legal, to handle those concerns.

Analyzing this prospective future in some detail (e.g., Section 4) provides handholds for the solutions that must be built if people are to achieve a modicum of privacy in the brave, new world of ubiquitous IoT. That means first understanding the privacy harms that can result from such smart devices in the home. It means developing threat models to capture the sequence of actions and inactions that would allow harm to occur. Most importantly, it means designing protections against those harms.

ACKNOWLEDGEMENTS

This research is supported by the National Science Foundation under award numbers CNS-1955805, CNS-1955228, and the Dartmouth College and American University of Kuwait (Dartmouth-AUK) fellowship program. The views and conclusions contained herein are those of the authors alone.

REFERENCES

[1] Syed Ishtiaque Ahmed, Shion Guha, Mohammad Rashidujjaman Rifat, Faysal Hossain Shezan, and Nicola Dell. Privacy vulnerabilities in the practices of repairing broken digital artifacts in bangladesh. *Information Technologies and International Development*, 2017.

[2] Wael S Albayaydh and Ivan Flechais. Exploring bystanders' privacy concerns with smart homes in jordan. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. Association for Computing Machinery.

[3] Ahmed Alshehri, Eugin Pahk, Joseph Spielman, Jacob T Parker, Benjamin Gilbert, and Chuan Yue. Exploring the negotiation behaviors of owners and bystanders over data practices of smart home devices. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, New York, NY, USA, 2023. Association for Computing Machinery.

[4] Ahmed Alshehri, Joseph Spielman, Amiya Prasad, and Chuan Yue. Exploring the privacy concerns of bystanders in smart homes from the perspectives of both owners and bystanders. *Proceedings on Privacy Enhancing Technologies*, 3:99–119, 2022.

[5] Noah Apthorpe, Dillon Reisman, and Nick Feamster. A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. *arXiv preprint arXiv:1705.06805*, 2017.

[6] Julia Bernd, Alisa Frik, Maritza Johnson, and Nathan Malkin. Smart home bystanders: Further complexifying a complex context. In *Proceedings of CI Symposium*, 2019.

[7] Cara Bloom, Stuart Shapiro, Benjamin Ballard, Shelby Slotter, Mark Paes, Julie McEwen, Ryan Xu, and Samantha Katcher. The panoptic privacy threat model. In *Proceedings of 30th ACM Conference on Computer and Communications Security (CCS'23)*. ACM, 2023.

[8] Sarah Brayne. Surveillance and system avoidance: Criminal justice contact and institutional attachment. *American Sociological Review*, 79(3):367–391, 2014.

[9] Sarah Brayne. Big data surveillance: The case of policing. *American sociological review*, 82(5):977–1008, 2017.

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

[11] Danielle Keats Citron and Daniel J Solove. Privacy harms. *BUL Rev.*, 102:793, 2022.

[12] Camille Cobb, Sruti Bhagavatula, Kalil Anderson Garrett, Alison Hoffman, Varun Rao, and Lujo Bauer. "I would have to evaluate their objections": Privacy tensions between smart home device owners and incidental users. In *Proceedings on Privacy Enhancing Technologies Symposium*, volume 2021, pages 54–75, 2021.

[13] Control4. Live Life Brilliantly, https://www.control4.com/, 2023.

[14] Diane J. Cook. How Smart Is Your Home? 335(6076):1579–1581.

[15] Sarah Delgado Rodriguez, Sarah Prange, Christina Vergara Ossenberg, Markus Henkel, Florian Alt, and Karola Marky. Prikey – investigating tangible privacy control for smart home inhabitants and visitors. In *Nordic Human-Computer Interaction Conference*, NordiCHI '22, New York, NY, USA, 2022. Association for Computing Machinery.

[16] Ayyoob Hamza, Hassan Habibi Gharakheili, and Vijay Sivaraman. Combining MUD Policies with SDN for IoT Intrusion Detection. In *Proceedings of the 2018 Workshop on IoT Security and Privacy - IoT S&P '18*, pages 1–7. ACM Press, 2018.

[17] Ayyoob Hamza, Dinesha Ranathunga, Hassan Habibi Gharakheili, Matthew Roughan, and Vijay Sivaraman. Clear as MUD: Generating, validating and applying IoT behavioral profiles. In *Proceedings of the 2018 Workshop on IoT Security and Privacy - IoT S&P '18*, pages 8–14, New York, New York, USA, 2018. ACM Press.

[18] Weijia He, Jesse Martinez, Roshni Padhi, Lefan Zhang, and Blase Ur. When smart devices are stupid: Negative experiences using home smart devices. In *2019 IEEE Security and Privacy Workshops (SPW)*, pages 150–155, 2019.

[19] William Jang, Adil Chhabra, and Aarathi Prasad. Enabling multi-user controls in smart home devices. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, IoTS&P '17, page 49–54, New York, NY, USA, 2017. Association for Computing Machinery.

[20] Eliot Lear, Ralph Droms, and Dan Romascanu. Manufacturer Usage Description Specification draft-ietf-opsawg-mud-22, 2018.

[21] Mikhail A Lisovich, Deirdre K Mulligan, and Stephen B Wicker. Inferring personal information from demand-response systems. *IEEE Security & Privacy*, 8(1):11–20, 2010.

[22] Anna Maria Mandalari, Daniel J. Dubois, Roman Kolcun, Muhammad Talha Paracha, Hamed Haddadi, and David Choffnes. Blocking Without Breaking: Identification and Mitigation of Non-Essential IoT Traffic. 2021(4).

[23] Shrirang Mare, Logan Girvin, Franziska Roesner, and Tadayoshi Kohno. Consumer smart homes: Where we are and where we need to go. In *Proceedings of the International Workshop on Mobile Computing Systems and Applications (HotMobile)*, pages 117–122. ACM Press, 2 2019.

[24] Sarah Prange, Sarah Delgado Rodriguez, Timo Doeding, and Florian Alt. "Where did you first meet the owner?" – Exploring Usable Authentication for Smart Home Visitors. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, pages 1–7, New York, NY, USA, 4 2022. ACM.

[25] Parth Kirankumar Thakkar, Shijing He, Shiyu Xu, Danny Yuxing Huang, and Yaxing Yao. "it would probably turn into a social faux-pas": Users' and bystanders' preferences of privacy awareness mechanisms in smart homes. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. Association for Computing Machinery.

[26] Maximiliane Windl and Sven Mayer. The skewed privacy concerns of bystanders in smart environments. *Proc. ACM Hum.-Comput. Interact.*, 6(MHCI), sep 2022.

[27] Jong-bum Woo and Youn-kyung Lim. User experience in do-it-yourself-style smart homes. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing - UbiComp '15*, pages 779–790, New York, New York, USA, 2015. ACM Press.

[28] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. Privacy perceptions and designs of bystanders in smart homes. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), nov 2019.

A HANDYTECH REALTY SCENARIO

The scenario includes the following roles: Seller, Buyer, Seller, HandyTech, Inspector. There is one key asset: Seller House.

Seller is a professional couple who are looking to move out of their current house and get a larger and more centrally-located house. Their current house, which we'll call *Seller House*, is equipped with a WiFi network and a wide range of IoT devices. These are sometimes linked together with IFTTT trigger rules over a diversity of sensors and actuators.

Buyer is an older couple who are just entering retirement. They have some technical knowledge, but little experience with (or interest in) IoT. When they made an offer for Seller House, they stipulated that IoT devices should be disabled and removed from the house as part of the transfer.

Buyer is advised by their realtor to get an inspection of the house by a professional house inspector. The realtor further recommends getting a HandyTech to look over the state of IoT devices and networking in the house. Realtor recommends a house inspector who is also a HandyTech and has substantial experience with IoT systems. We call this party *Inspector* from now on.

As part of the transfer preparations for the transfer of Seller House, Inspector gets in touch with *Seller HandyTech* to work out plans for conforming to the terms of the sale. Seller HandyTech conducts a fresh inventory of the IoT devices in Seller House and passes this along to Inspector. Inspector confirms expectations like removing all IoT cameras in the Seller House, and assisting the Inspector in confirming that, up to customary standards of care, the wishes of the Buyer have been met. This is duly reported to Buyer and confirmed in the final walkthrough of the sale.

Variant 1: In the first variant of this scenario, Buyer wants to keep some IoT devices and use their data. These are selected from the inventory by Buyer in consultation with Inspector. It is agreed to turn over the thermostat along with an AI prediction model that was learned from the Seller House while it was occupied by Seller. Inspector and Seller HandyTech explain to Buyer and Seller what this might mean for information flows, such as potentially exposing facts about Seller habits to Buyer.

Variant 2: Inspector finds that there is an array of sensors in the basement of Seller House that log humidity and leaks. The Buyer's Inspector asks to have these logs, and Seller HandyTech agrees. These sensor logs show a gap during the summer of the previous year during a period of heavy rains and flooded homes in the area. The Buyer asks for an explanation for the information gap; the

Sellers say they don't know but admit there was some water in the basement twice during the flooding period. The Buyer renegotiates the sale for a reduction in price to cover the costs of sump pump and some regrading around the house.

Variant 3: The Seller's HandyTech is asked to represent both Seller and Buyer in the inspection. Buyer knows the company that employs Seller HandyTech and trusts them to maintain objectivity in the inspection process, but the Handyperson Code of Ethics prevents the same HandyTech from working for Buyer and Seller during such a transaction. Instead, the Buyer's realtor finds a new HandyTech who is employed by the Buyer to do the home inspection. Once the real-estate transaction is completed, the Buyer hires the Seller's HandyTech.