We Need a "Building Inspector for IoT" When Smart Homes Are Sold

Timothy J. Pierson and **Cesar Arguello** | Dartmouth College
Beatrice Perez | University of Massachusetts Boston
Wondimu Zegeye and **Kevin Kornegay** | Morgan State University
Carl A. Gunter | University of Illinois, Urbana-Champaign
David Kotz | Dartmouth College

Internet of Things (IoT) devices left behind when a home is sold create security and privacy concerns for both prior and new residents. We envision a specialized "building inspector for IoT" to help securely facilitate transfer of the home.

Roughly 6 million homes are sold each year in the United States alone.[1] Before a home is sold, a building inspector often examines the integrity of the building and renders an opinion on its soundness—examining things like structural integrity, electrical safety, mold and mildew, and radon or other toxins. These inspectors have specialized tools, knowledge, and experience to make a more informed judgment than nonprofessionals are capable of making.

Introduction

Because of the expected explosion in the presence of Internet of Things (IoT) devices in homes, we highlight the need for a new professional—a *home IoT inspector*—to aid in the transfer of a home to new residents when the home is sold. Similar to the building inspector, the home IoT inspector is equipped with specialized tools, knowledge, and experience to examine a home's IoT infrastructure prior to completion of a sale. We envision that the home IoT inspector would examine a home after the prior residents move out and before the new residents take possession. The inspection would create an inventory of *all* smart things (IoT devices) left behind in a home by the previous residents, wipe any data or credentials pertaining to the previous residents, and facilitate transfer of control of the home's devices to the new residents.

In this article, we make the case for this new profession and emphasize the challenges of selling a smart home in the near future. We believe these challenges have not been thoroughly investigated in the literature, and that problems transferring home ownership will become worse in the future as the number of deployed smart devices grows. Our goal in this article is not to report on specific experiments but rather to elucidate problems that will likely arise when smart homes are sold, to highlight open research questions, and to sketch the outlines of a new profession. We hope this article will generate discussions that ultimately lead to real-world deployable systems.

More Devices, More Problems

IoT devices that have computational and communication capabilities are becoming increasingly common in homes, and the number of these deployed "smart" devices is expected to grow rapidly in the next few years.[2] If these predictions are correct, in the near future there may be dozens (or even hundreds!) of IoT devices in many homes. For example, designers are experimenting with smart forks to detect and log what people eat.[3] If each piece of silverware becomes smart, and if other

Digital Object Identifier 10.1109/MSEC.2024.3386467
Date of publication 7 May 2024; date of current version 11 November 2024.

Figure 1. Homes in the near future may contain dozens or even hundreds of IoT devices. When a home is sold to a new owner, some devices may be left behind by the prior residents. These devices will need to be inventoried, the personal information and device access of prior residents must be removed, and control of the devices must be transferred from the prior residents to the new owner. These steps will likely become increasingly difficult as the number of IoT devices in the home increases. We propose a *home IoT inspector* to help facilitate these steps.

historically nonsmart items similarly become smart, we could easily see orders of magnitude more devices in homes than are typically present today.

Figure 1 illustrates such a home, highlighting the numerous smart devices present in just a single room. Each of these devices may observe and log some portion of its local environment. In aggregate, these logs may reveal a significant amount of personal information about the characteristics and behavior of home residents, raising important security and privacy challenges.

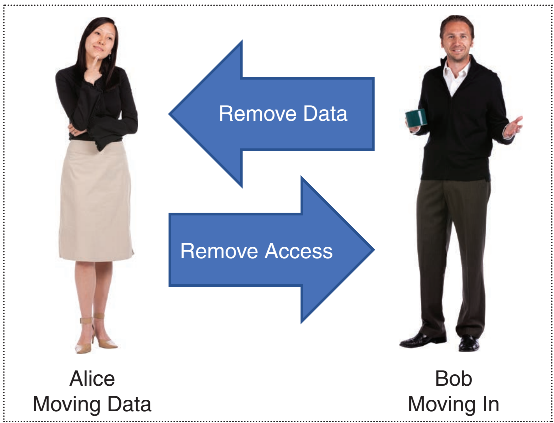


Figure 2. If Alice moves out of a home and Bob moves in, security and privacy must be maintained in both directions. Sensitive data must be removed from devices left behind so Bob cannot learn about Alice, and Alice's access must be removed from devices now used by Bob so she cannot learn about him or control aspects of his home.

These challenges are particularly salient when a home is sold to a new owner because some devices may be left by the prior residents as part of the sale (for example, major appliances and systems for lighting, heating, cooling, and security—all of which are increasingly connected to the Internet and to cloud services). These devices will likely be used by the new residents.

Threat Model

In this article, we consider the threats to both the prior as well as the new residents. While there are many potential actors, we are primarily concerned with the interaction of these two stakeholders and how they may pose threats to each other. Importantly, the privacy and security issues are bidirectional, as shown in Figure 2. That is, the prior residents must be protected from the new residents, and the new residents must be protected from the prior residents. For example, if Alice is moving out of a home and Bob is moving in, Alice must be protected so Bob does not learn sensitive information about Alice by examining data on devices she left behind—or leveraging credentials on those devices to access Alice's information in the cloud. This situation suggests that at least some data on those devices should be thoughtfully removed. Likewise, Bob must be protected from Alice. Alice's access to devices now used by Bob should be removed so that she is not able to control Bob's devices or see data produced by those devices.

Here we do not consider other threat actors, such as outside adversaries attempting to passively observe home network traffic to learn about the resident's behavior and preferences, nor do we consider active adversaries that attempt to inject traffic or otherwise disrupt systems in the home. While those threats are important, we limit our discussion to the interaction between prior and new residents.

Sensitive Data

When we refer to sensitive information, we mean data that could potentially lead to harm or other negative consequences for either the new or prior residents. Solove provides a well-known taxonomy of harms[4] that includes 1) information collection, 2) information processing, 3) information dissemination, and 4) invasion. In this article we focus on *information collection* from devices located in the home. Sensitive data include multimedia data (such as video and audio recordings), authentication credentials, user behavioral information (for example, inferences derived from network traffic, sensor readings, or device access times/frequency), and user preferences (for example, inferences derived from data such as specific movies watched or browser history).

Identifying specifically which data are sensitive can be context dependent and can vary significantly between residents.[5] These attitudes should be considered when transferring ownership of a smart home.

The Home IoT Inspector

We envision the home IoT inspector as a technically skilled individual with specialized tools, knowledge, and experience. The home IoT inspector's function is to prepare smart homes for ownership transfer. The home IoT inspector may be licensed by government agencies or professional societies, and as such could be bonded to ensure he/she does not divulge private information. One IoT inspector could be retained by the buyer, and a different inspector could be retained by the seller—like realtors today—but for simplicity we assume both the buyer and seller agree to one IoT inspector.

Device Types

Before discussing the tasks that must be accomplished to transfer a smart home from the prior residents to the new residents, we first contemplate the types of devices that must be accommodated in the transfer.

Devices Not Intended to Be Left Behind

Many IoT devices are primarily operated by a single person. For example, cellphones, tablet computers, laptops, and fitness trackers are not commonly shared. Over time, these devices can accumulate information about the operator that could cause privacy or security harms if that information were exposed. A browser history, for example, could tell an adversary a great deal about a person's interests and tastes. GPS locations could reveal frequent routes of travel. While these details are important, personal devices will likely be taken with the residents when they vacate a home and move to a new one.

Other devices, such as an Amazon Alexa, may not be personal devices, but instead may be considered communal devices, shared by multiple residents. These devices may also contain sensitive data about each of their users.

An important consideration, however, is that if the home contains dozens or hundreds of devices, it could be easy for residents to mistakenly leave a device behind that they intended to take with them, especially if the device is not considered a personal device by any resident. Ideally, there would be a means for the departing residents to "double-check" that they have all of the devices they intend to take when they leave.

Devices Purposely Left Behind

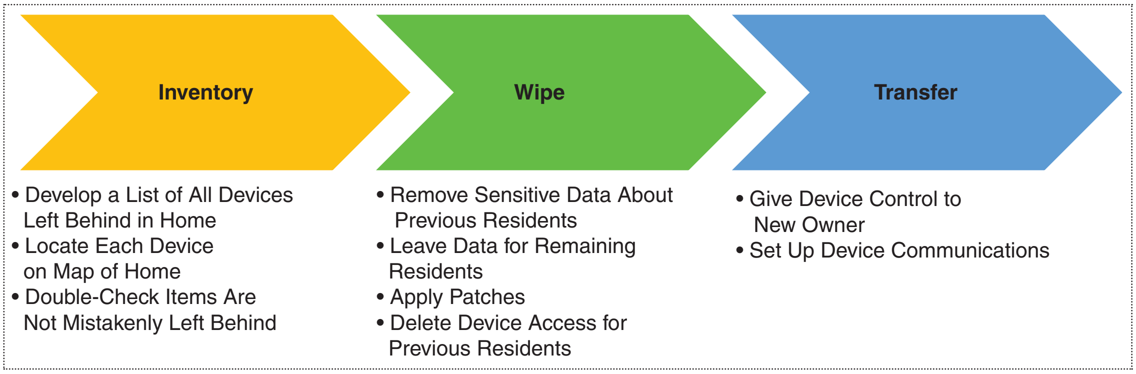
Some devices may be purposely left behind in a home when residents move out. In this section, we highlight some of those devices.

Home infrastructure devices. Some devices may be considered as part of the home's infrastructure and may remain in place when the current residents move out. These devices do not typically belong to a single person but generally serve all residents and guests. Appliances like smart refrigerators or laundry machines are often sold as part of the house. Built-in devices, like smart thermostats and the building's heating, ventilation, and air conditioning system, are typically embedded and expected to be part of the sale. Similarly, security devices, such as cameras, motion sensors, and smart door locks, may also remain in place. These devices may contain sensitive historical information about the prior residents that should be removed so that new residents do not learn about the characteristics and behaviors of the prior residents. As we have noted, the bidirectional nature of the home IoT means that access to these devices should also be removed so that the previous residents are no longer able to control the home's devices or learn anything about the new residents.

> **"In aggregate, these logs may reveal a significant amount of personal information about the characteristics and behavior of home residents, raising important security and privacy challenges."**

Devices not owned by residents. Some devices present in a home may not belong to a resident. A landlord, for example, may install and operate devices such as temperature and water leak sensors. To protect the prior residents' privacy, sensitive data about the prior residents should be removed from these devices, even though they are not owned or operated by any resident of the home. We discuss multistakeholder considerations in more detail in the section "Complicating Factors."

Malicious devices. Sometimes people install malicious devices, such as hidden cameras or microphones. These devices may be purposefully concealed to allow the prior resident to covertly monitor the new



Inventory

- Develop a List of All Devices Left Behind in Home
- Locate Each Device on Map of Home
- Double-Check Items Are Not Mistakenly Left Behind

Wipe

- Remove Sensitive Data About Previous Residents
- Leave Data for Remaining Residents
- Apply Patches
- Delete Device Access for Previous Residents

Transfer

- Give Device Control to New Owner
- Set Up Device Communications

Figure 3. Three tasks must be performed when a home is sold. The first is to create a comprehensive inventory of devices left behind and a map of their location on a floorplan. This inventory can be used by the prior residents to "double-check" that items are not accidentally left behind and by the new residents to ensure they have received all expected devices and understand their location. The second task is to remove all sensitive data and credentials about the prior residents and to remove device access by previous residents. Optionally, the inspector may take the opportunity to patch devices to close any open security holes or to update functionality. Finally, the new residents are given control of the devices.

resident. All of these devices should be discovered and removed before new residents take possession of the home.

Tasks Required When a Home Is Sold

As highlighted previously and shown in Figure 3, three primary tasks must be completed to protect both prior and future residents' security and privacy: 1) ensure that the *inventory* of smart devices left in the home matches what is expected according to the sales agreement, 2) *wipe* sensitive data about prior residents from those devices, and 3) *transfer* control of those devices to the new residents. Although it may be possible for a nonprofessional to accomplish each of these tasks today, it will be increasingly difficult as the number and variety of IoT devices in a home grows. At some point, professional help will be required for many people.

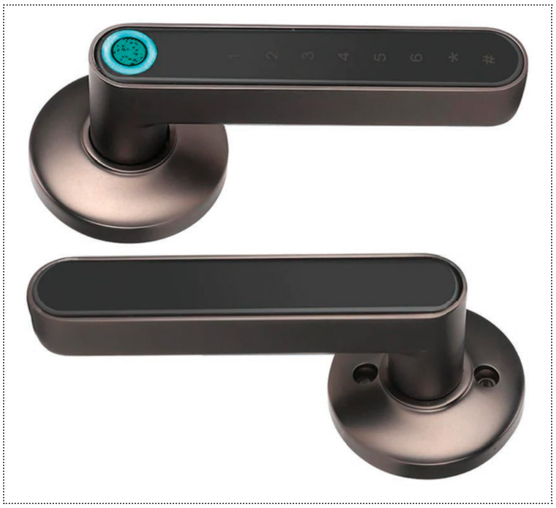


Figure 4. A door handle that appears to be an ordinary handle until the sensor is activated.[6] Devices like this one could be easily overlooked in a visual search. It could also be missed by network sniffers if it does not transmit often (perhaps only when a door opens). Finally, it may not respond to any device discovery protocol. The result is that this device, and others like it, may not be listed in an inventory of devices in a home.

Ensure the Inventory of Smart Devices Left in the Home Matches What Is Expected According to the Sales Agreement

Ideally, this task would produce a comprehensive list of all devices, their type, their purpose, and their physical location within the home. This inventory can help prior residents double-check that they have not left any devices they intended to take. It can also help the new residents ensure the home contains nothing less, and nothing more, than what they expected to be included in the sale. We outline several device discovery approaches, each with drawbacks that make developing a comprehensive device inventory difficult.

Visual search. One naive approach is a simple visual search, noting the type and location of each device. This approach fails for four reasons. First, while some devices remaining in the home will be easy to visually spot, others will be more difficult. For example, Figure 4 shows a smart door lock that appears to be a "dumb" door handle. It is not until the lock is activated that it becomes apparent that this is a smart device. Second, some devices, such as security cameras, may be purposely hidden to avoid visual detection. Third, some smart devices may be built into the structure of the home—embedded in the walls, floors, or ceilings. Finally, the large number of devices expected to be present in many smart homes will make developing a comprehensive inventory from a visual search time-consuming and error-prone.

Sniffing. Another approach to discover devices in a home is to sniff network traffic and record devices based on an identifier such as a media access control address or by patterns in their communications. Sniffing is difficult if the goal is to discover *all* devices, however. First, a sniffer must be aware of all communication protocols used by devices in the home. A Wi-Fi sniffer will not detect Bluetooth or Zigbee devices. Second, a sniffer must listen on all frequencies used by devices in the home. Wi-Fi has two bands (2.4 and 5 GHz) and multiple channels within each band. A sniffer operating on one channel will not detect devices communicating on another. Third, in larger homes it may not be possible for a single sniffer, in a single location, to receive wireless transmissions from all possible locations in or around the home. Furthermore, some devices may communicate infrequently (possibly only when triggered by an event such as motion detected or a door opening), making sniffing difficult. Others may communicate only over a wired connection, making wireless sniffing impossible. Finally, a sniffer capable of detecting digital communications may not be able to detect analog communications or devices that attempt to hide their presence, such as a security camera that records data to a memory card that is later physically retrieved.

Sniffers may be able to discover a large number of devices left behind, but they are unlikely to discover all of them.

Device discovery protocols. Researchers have proposed device discovery protocols in which devices respond to some type of inquiry message with information about them (see Achir et al. for a survey[7]). These approaches work well if the devices can be trusted to respond with truthful information. Malicious devices may not respond to the discovery inquiry (or the malicious device may lie about its identity or type). Other devices may not be aware of the discovery protocol and may not know how to respond. In these cases, device discovery protocols may not find all devices left in the home. Furthermore, as with sniffing, the device discovery protocol would need to operate on all types of communication protocols used by devices in the house, but device discovery protocols typically only work with one protocol (for example, Wi-Fi but not Bluetooth). If the device discovery protocol does not cover a particular communication modality, some devices may not be detected.

Harmonic radar. A promising new approach proposed by Perez et al. uses harmonic radar to discover the presence of electronics in homes.[8] It works by transmitting a radio frequency using a highly directional antenna and listening for a nonlinear response caused by electronic components, such as transistors and diodes. Unlike a sniffer, this method detects the presence of electronic devices irrespective of the device's communication protocols and does not require the device to respond to a discovery inquiry. It even works if the device is powered off! Recent work has shown that device types can be identified with high accuracy (for example, the harmonic radar can determine the specific model of a camera) from a set of known devices.[9]

A key limitation of harmonic radar, however, is its short range. Harmonic radar has been demonstrated to be capable of detecting consumer electronics at distances up to 2 m, which is clearly insufficient when the goal is to find all devices in a home.

Home IoT inspector's inventory role. Because there is no existing tool that can comprehensively discover *all* devices in a home, we imagine the home IoT inspector using a combination of device discovery approaches to ensure that every device in the home is identified, localized, and inventoried. For example, the home IoT inspector might temporarily install a sniffer to detect transmitting devices and might use a portable harmonic radar to manually sweep the home to discover other devices. The home IoT inspector might then use the list of discovered devices to visually inspect each one, noting its location and type. The home IoT inspector could also confer with the prior residents and use their domain knowledge to infer the device's purpose in the home. In the end, the home IoT inspector would produce a comprehensive inventory of devices remaining in the home.

Wipe Sensitive Data About Prior Residents From Devices

Once an inventory is complete, all remaining devices must be wiped. The goal is to erase any sensitive data or configurations that would allow the new residents to infer private information about the previous residents. The data might be contained in the device itself or, alternatively, the device may contain credentials that connect to a cloud service where sensitive data may reside. Additionally, the prior resident's access to the device should be removed.

One might argue that a simple solution to wipe sensitive data is to physically visit each device and do a factory reset (assuming the device even has such a capability!). There are, however, three problems with this approach.

Some user data should be retained. In some cases, some data should be retained on each device. When one roommate moves out, but others stay, only data from the departing roommate should be removed. If the device were reset, each remaining roommate would need to recreate his/her settings for each device. This might entail reentering local settings as well as cloud-based resource credentials. Aside from the inconvenience and time required, remembering all of these credentials can be difficult, especially if the residents do not reuse usernames and passwords.

Patches and upgrades may be lost. Ideally, devices are updated as new security and functionality patches become available. A factory reset may remove these updates. Ideally, devices are fully patched and prepared for duty when they are transferred to new resident.

Communication with other devices would need to be reset. Some devices interact with other devices within the home. Consider a device that remains, as part of the sale of the home, while other devices move out. Suddenly, some of the devices with which a device expects to interact—and perhaps even on which it depends—are gone. A factory reset on all of the remaining devices might cause this device and its remaining "partners" to forget those relationships. These cross-device connections and relationships need to be reestablished. If there are dozens or hundreds of devices in the home, and some percentage of them are left behind, reinitiating each of these connections could be a time-consuming and error-prone process.

Home IoT inspector's data wipe role. Identifying exactly what data can be used for privacy-impinging inference is difficult. Many clever techniques have been developed that use seemingly innocuous data to learn a great deal more than might be anticipated. For example, Kounoudes et al. showed that surprisingly detailed home-occupant behavior can be identified using seemingly unimportant data from a simple IoT water flowmeter.[10] It might not be readily apparent to a nonexpert user that logs from the water flowmeter should be erased. A comprehensive inventory of devices left behind, however, can give an expert home IoT inspector clues about what should be addressed.

We envision the inventory acting somewhat like a checklist of things for the home IoT inspector to consider. The home IoT inspector would review each item on the inventory and consider what data it may hold and the security and privacy implications of leaving those data on the device. The home IoT inspector may also interview the residents to understand their security and privacy preferences. The home IoT inspector can then use their judgment and experience to determine the data that should be removed on each device. The inventory helps to ensure they do not forget to address any devices (even the water flowmeter in the basement).

After determining the specific data that should be removed from each device, a further challenge is to take the necessary steps to remove those data. The specific process that must be followed will vary widely in a home populated with many smart devices from heterogeneous vendors. Currently, there is no universal approach for identifying and removing sensitive information on all IoT devices. A nonexpert user may not have the knowledge or patience to take the necessary actions on each device. A trained home IoT inspector—who is equipped with specialized tools and who is able to attest that the data were deleted—may be more effective.

Finally, after wiping each device, the home IoT inspector may apply any needed patches. After this step, the devices are fully prepared for the new residents.

Transfer Control of Devices to the New Residents

The final step is to transfer control of the remaining devices to the new residents. The goal is to make sure the new residents are able to control the devices in the home and ensure the previous residents cannot. That is, one must ensure the new residents have administrator capabilities on all devices so that they can reconfigure the devices as they desire, but the prior residents cannot. Currently, there are no systematic solutions that will transfer control from the prior residents to the new residents across a large number and variety of devices left behind. For individual devices, the literature includes several approaches, including using cryptographic methods[11] or blockchain[12] technology, but many existing IoT devices will not conform to these approaches, and it is unlikely that all future IoT devices will either. This situation suggests there is a need for judgment (based on experience) to ensure all devices in a home are securely transferred to the new residents.

Home IoT inspector's transfer role. Using the inventory as a guide, the home IoT inspector would work with the new residents to configure devices according to their preferences. This step may help alleviate issues where the new resident may not be familiar with the prior residents' specific devices. If the home IoT inspector is also not familiar with a particular device, he/she could be paid to assist—to read the device manual or call the manufacturer's help desk. The home IoT inspector can also help set up communications between the new residents' devices and the devices that were left behind and link the devices to the new residents' cloud services where necessary.

Home Sales Without an IoT Inspector

There are several possible ways to facilitate transfer of a home containing numerous smart devices. In this section, we highlight a continuum of approaches without using a home IoT inspector. These approaches range from those available today to methods that rely on technologies that may evolve at some point in the future. We also highlight several open research questions.

Residents Handle the Transfer Themselves

The prior and new residents may cooperate among themselves to handle the three primary tasks: inventory, wipe, and transfer. This approach is what commonly happens today, and it requires the least amount of assistive technology. This approach, however, is likely to be the most error-prone, especially if one or both of the residents are not tech savvy.

Inventory. The prior residents operate most devices within their home (possibly alongside devices owned by a landlord), so it may seem reasonable to assume the residents already have a complete inventory of their devices. This assumption may have been historically true, but as the number of devices in the home grows to dozens or even hundreds, this assumption becomes less certain. It will be easy for residents to forget some devices, such as the out-of-sight (and possibly out-of-mind) basement water flowmeter mentioned previously.

Wipe. Next, the prior resident will need to wipe data on each of the devices that will remain in the home. Because there is no universal protocol to securely remove all sensitive information from devices, the resident moving out will need the skill and inclination to not only identify what should be removed, but also to ensure no traces remain on the devices. Many residents will not have these skills. Even those who do possess the required skills may not have the time or inclination to wipe every device, particularly when also dealing with the other logistical nuisances that occur during a home move, such as packing, arranging for movers, unpacking, and so forth.

Even assuming the previous residents did wipe their data, would the new resident be willing to trust that access to the device was also removed? The new resident would have to believe that 1) the prior resident did the work, and 2) the prior resident had the skill and diligence to do the work *well*. Answer: The new resident should not trust the previous resident; hence, the need for a trusted third party, the home IoT inspector.

Transfer. Finally, the new resident will need to assume administrative control over each device. In some way the new resident must learn credentials, such as usernames and passwords for each device. Currently, the only widely available options are a device factory reset (which is often undesirable, as discussed in the section "Tasks Required When a Home Is Sold") or having the prior resident inform the new resident of each device's credentials, revealing information about the prior resident's (possibly reused) passwords.

Additionally, the new resident may not be familiar with the specific make and model of a device left behind. In that case, the new resident faces the time-consuming task of reading device manuals or interacting with the manufacturer's service desk to remove access. It would be easy to make a mistake configuring an unfamiliar device.

Open research questions. Even assuming a situation with well-intended and technically knowledgeable residents, cooperation between the prior and new residents is an error-prone process. This problem is likely to get worse as more devices are deployed. Open research topics include the following:

- How can *all* devices in a home be identified, inventoried, and accurately localized? How can a residence's device be identified in dense living situations, such as apartment buildings where wireless transmissions from neighbor's devices pass into the residence? How can all frequencies and communication protocols be covered?
- How can sensitive information be removed from devices while maintaining other data such as credentials to communicate with other remaining home devices? How can the prior residents be sure they have removed *all* sensitive data from *every* device?
- How can the new resident easily assume administrative control over all devices?
- How can a new resident's devices be integrated with the devices left behind by the prior resident? What about compatibility issues? For example, suppose the prior residents used devices primarily from one vendor (Google, for example), and the new residents use devices from another vendor (say, Apple). What if some devices depend on another device that is no longer present after the prior residents move out and take some devices with them (say, for example, a smart door lock depends on a home-security hub that was removed as part of the move)?

- How should the home transfer happen if one or both residents are not technically savvy? What if one or both residents are uncooperative or even adversarial (in a case of domestic violence, for example)?
- What should happen if one or more residents remain in the residence while others move out? What if the resident moving out was the person who primarily managed the home's devices, and the remaining resident is less knowledgeable?

These open questions suggest that in many cases the prior and new residents will have difficulty transferring the smart home. An automated solution might help. Next we discuss two such possibilities that do not exist today but might evolve in the intermediate and long run. We contend, however, that in the short run and possibly longer, a dedicated human professional can help solve these problems.

Automated Smart Home Transfer Agent

New technologies might evolve to facilitate inventory, wipe, and transfer control of all smart devices in a home. An automated smart home transfer agent might be somewhat similar to smart agents who help transfer software when a user buys a new computer. These agents inventory the software installed on the old computer and facilitate installation on the new computer. Until such an automated system exists for a smart home IoT, a skilled IoT inspector is required.

If such a smart home transfer agent were developed, it may be the case that manufacturers develop a system for their devices, but it is unlikely that the agent will handle every manufacturer's devices. Even in the future world where the smart-home transfer agent exists, the residents are still left dealing with multiple solutions if the home is populated by devices produced by multiple vendors.

Open research questions. The smart transfer agent would need to solve several open research questions, including:

- How will the transfer agent function if there are devices from multiple manufacturers? What about smaller manufacturers that do not provide a transfer agent for their devices?
- How will the agent know what information is sensitive? How will it remove only those sensitive data? How will it attest the data are actually removed?
- How will the agent configure devices for the new residents? How will it learn their preferences?
- How can the residents trust that the agent acted in accordance with their wishes or preferences?
- Few homes are exactly alike. How will this agent deal with all the idiosyncrasies in a home?

Artificial Intelligence-Based Agent

Finally, we can imagine a superintelligent artificial intelligence (AI)-based agent. While the previous solution we described was somewhat "intelligent." we envision it to be unable to reason about its environment or make nuanced decisions that account for resident preferences. Now we envision a more capable solution that, similar to a human, is able to account for all of the idiosyncrasies in a home. This agent could potentially introduce new devices to the home's infrastructure (for example, provide access credentials once the new device has been identified and authenticated). The agent would thus have an accurate inventory of the home's devices and would know the credentials of each device because it introduced each new device to the home. The AI-based agent could then selectively wipe the sensitive data on each device, remove the prior resident's access, and grant administrative control to the new resident (or perhaps the new resident's AI agent).

Open research questions. The following questions come to mind:

- When should a human be in the loop to verify that the AI's decisions are correct?
- What skills would the human need?
- What if the human disagrees with the AI?

This AI-based scenario is appealing, but it appears to be on the distant horizon. In the meantime, we need a practical solution for the near future. We propose a human home IoT inspector with specialized tools and knowledge for the short and intermediate future. If the AI-based agent is developed, it might lessen or replace the need for a human to help transfer smart homes.

Complicating Factors

Until now we have primarily assumed all residents moved out of a home and the new residents take control after a sale. In reality things are often more complicated.

Other Stakeholders

Sometimes there are other stakeholders in addition to the residents. In a rental property, the landlord owns the home, but the tenants may change when a lease expires. In this case, the same tasks discussed previously apply, but the home IoT inspector may temporarily transfer control back to the landlord when tenants move out. For example, suppose an apartment includes a smart refrigerator that remains with the apartment when the lease ends. When the tenants depart, the home IoT inspector wipes any personal information, removes access from those tenants, and transfers control back to the landlord. When a new tenant moves in, the home

IoT inspector might help facilitate control of the fridge from the landlord to the new tenant.

Not Everyone Moves Out

Some devices may be owned by one resident but shared by multiple people. These devices create a conundrum if some residents move out, but other residents stay. Imagine, for example, that Carol and Dave are roommates and share a smart TV owned by Carol. Dave moves out, but Carol stays. Data on the smart TV about Dave's preferences should be removed, but Carol's should remain because she still uses the TV. In this case, some but not all data should be removed. A simple factory reset is not desirable because it would erase Carol's personal settings and any communication with other home devices, such as a Wi-Fi access point, and would also reset communication with any cloud services Carol uses.

Other Situations

In some cases, tenants change frequently, such as in hotels and Airbnb rentals. We envision that a modified version of our approach could be employed to allow the new guests to easily take control of all smart devices in the temporary quarters (perhaps with a single set of credentials) but allow the landlord to automatically resume control when the tenants leave. After the guest departs, housekeeping staff might use the system to ensure all expected devices remain in the room.

It could also be the case that the landlord grants access to some device functionality but retains administrative control. An example could be a senior housing facility where residents are allowed to control devices, such as adjusting a thermostat within preset limits, but residents are unable to change the device's password.

In this article we describe some of the challenges that arise when selling a smart home. Historically, homes have not included smart devices—at least, not as part of the home when it is sold—and protecting the privacy of both the prior and new residents has not been difficult. Given current trends, homes of the near future may soon contain dozens or even hundreds of smart devices. Preparing a home for sale in that case will be significantly more difficult. We believe a kind of "building inspector" is needed to protect both the prior and the new residents. This new professional *home IoT inspector* will have specialized tools, training, and experience, not unlike a building inspector of today. ■

Acknowledgment

This research results from the SPLICE research program, supported by a collaborative award from the SaTC Frontiers program at the supported by the National Science Foundation under awards CNS-1955805, CNS-1955172, CNS-1955228, and CNS-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 the sponsors. Any mention of specific companies or products does not imply any endorsement by the authors, by their employers, or by the sponsors.

The authors are grateful for the insightful guidance provided by Denise Anthony, Adam Bates, Susan Landau, Michel Kornegay, Michelle Mazurek, and Avi Rubin.

References

1. "Number of existing homes sold in the United States from 2005 to 2023." Statistica. Accessed: Mar. 8, 2024. [Online]. Available: https://www.statista.com/statistics/226144/us-existing-home-sales/
2. "IoT value set to accelerate through 2030: Where and how to capture it." McKinsey & Company. Accessed: Apr. 22, 2023. [Online]. Available: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it
3. "Hapifork bluetooth-enabled smart fork." Hapifork.com. Accessed: Apr. 22, 2023. [Online]. Available: https://www.hapilabs.com/product/hapifork
4. D. J. Solove, "A taxonomy of privacy," *Univ. Pennsylvania Law Rev.*, vol. 154, no. 3, pp. 477–564, 2006, doi: 10.2307/40041279.
5. W. He et al., "Rethinking access control and authentication for the home internet of things (IoT)," in *Proc. USENIX Secur. Symp.*, Berkley, CA, USA: USENIX Association, Aug. 2018, pp. 255–272.
6. "Fingerprint smart door lock." The Connected Shop. Accessed: Apr. 22, 2023. [Online]. Available: https://theconnectedshop.com/products/fingerprint-door-lock
7. M. Achir, A. Abdelli, L. Mokdad, and J. Benothman, "Service discovery and selection in IoT: A survey and a taxonomy," *J. Netw. Comput. Appl.*, vol. 200, Apr. 2022, Art. no. 103331, doi: 10.1016/j.jnca.2021.103331.
8. B. Perez, G. Mazzaro, T. J. Pierson, and D. Kotz, "Detecting the presence of electronic devices in smart homes using harmonic radar technology," *Remote Sens.*, vol. 14, no. 2, 2022, Art. no. 327, doi: 10.3390/rs14020327.
9. B. Perez, T. J. Pierson, G. Mazzaro, and D. Kotz, "Identification and classification of electronic devices using harmonic radar," in *Proc. 19th Int. Conf. Distrib. Comput. Smart Syst. Internet Things (DCOSS-IoT)*, Pafos, Cyprus. Piscataway, NJ, USA: IEEE Press, 2023, pp. 248–255, doi: 10.1109/DCOSS-IoT58021.2023.00050.
10. A. Dini Kounoudes, G. M. Kapitsaki, I. Katakis, and M. Milis, "User-centred privacy inference detection for

smart home devices," in *Proc. IEEE SmartWorld Ubiquitous Intell. Comput. Advanced Trusted Comput. Scalable Comput. Commun. Internet People Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI)*, Atlanta, GA, USA, Oct. 2021, pp. 210–218, doi: 10.1109/SWC50871.2021.00037.

11. Z. Wang, H. Ding, J. Han, and J. Zhao, "Secure and efficient control transfer for IoT devices," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 11, 2013, Art. no. 503404, doi: 10.1155/2013/503404.
12. J. Panduro-Ramirez, M. Lourens, A. Gehlot, D. P. Singh, Y. Singh, and D. J. Salunke, "Blockchain approach for implementing access control in IOT," in *Proc. Int. Conf. Artif. Intell. Smart Commun. (AISC)*, Greater Noida, India. Piscataway, NJ, USA: IEEE Press, 2023, pp. 596–599, doi: 10.1109/AISC56616.2023.10085452.

Timothy J. Pierson is a research assistant professor in the Department of Computer Science at Dartmouth College, Hanover, NH 03755-3529 USA. His research interests are in privacy and security, the Internet of Things, and applied machine learning. Pierson received a BS in computer science from Michigan Technological University and an MBA and a Ph.D. from Dartmouth College. He is a Member of IEEE. Contact him at timothy.j.pierson@dartmouth.edu.

Cesar Arguello is a computer science Ph.D. student at Dartmouth College, Hanover, NH 03755-3529 USA. His research interests include different aspects of cybersecurity, such as side-channel analysis, wireless network security, and exploitation of systems. Arguello received a BS in physics and computer science from the University of Florida. He is a Student Member of IEEE. Contact him at carguello.gr@dartmouth.edu.

Beatrice Perez is a research scientist at Riverside Research Institute in Lexington, MA, and a lecturer at The University of Massachusetts, Boston, Boston, MA 02125 USA. Her research interests focus on exploring the sensing capabilities of radio waves, particularly as they are used to detect, locate, and identify electronic devices. Perez received a Ph.D. from University College London, working with Prof. Mirco Musolesi and Gianluca Stringhini. She is a Member of IEEE. Contact her at bperez@riversideresearch.org.

Wondimu Zegeye is a postdoctoral researcher at Morgan State University, Baltimore, MD 21251 USA. His current research topics are machine learning and artificial intelligence for cybersecurity applications, such as intrusion detection systems, quantitative risk measurement, smart home security and privacy, and the Industrial Internet of Things. Zegeye received a BS in electrical and computer engineering from Addis Ababa University, Ethiopia, an MS in computer and communication network engineering and a Level II MS in future broadband networks from Politecnico di Torino, Italy, and a Ph.D. in electrical engineering from Morgan State University. He is a Member of IEEE of the Baltimore Section. Contact him at wozeg1@morgan.edu.

Kevin Kornegay is the Eugene DeLoatch Endowed Professor and director of the Cybersecurity Assurance and Policy Center at Morgan State University, Baltimore, MD 21251 USA. His research interests include system-on-chip design, hardware assurance, and secure embedded systems. Kornegay received a BS in electrical engineering from Pratt Institute, Brooklyn, NY, and an MS and Ph.D. in electrical engineering from the University of California at Berkeley. Dr. Kornegay is a Fellow of the American Association for the Advancement of Science and a Senior Member of IEEE. Contact him at kevin.kornegay@morgan.edu.

Carl A. Gunter is George and Ann Fisher Distinguished Professor in Engineering in the Computer Science Department of the University of Illinois at Urbana-Champaign, Urbana, IL 61801 USA. He is the director of the Illinois Security Lab, lead of the Genomic Security and Privacy Theme at the Institute for Genomic Biology, and founding chair for the Security and Privacy Area of the Department of Computer Science. His recent research focuses on security and privacy issues for the electric power grid and health-care information technologies. Gunter received a BA from the University of Chicago and a Ph.D. from the University of Wisconsin at Madison. He is a Member of IEEE. Contact him at cgunter@illinois.edu.

David Kotz is the provost and the Pat and John Rosenwald Professor in the Department of Computer Science at Dartmouth College, Hanover, NH 03755-3529 USA. His current research involves security and privacy in smart homes and wireless networks. Kotz received his AB in computer science and physics from Dartmouth College and his Ph.D. in computer science from Duke University. He is a fellow of the Association for Computing Machinery, a Fellow of IEEE, a 2008 Fulbright Fellow to India, a 2019 visiting professor at ETH Zürich, and an elected member of Phi Beta Kappa. Contact him at david.f.kotz@dartmouth.edu.