Who Or What Has Control Of Your Smart Home?

Description

Smart home technology has hidden dangers that most home owners do not understand. “Smart home” includes programmable devices within the home and, bi-directional connectivity to the Internet. Utility smart meters provide another gateway to monitor and control connected electrical devices such as thermostats, refrigerators, washers and driers, etc. ? TN Editor

On the first night in his new home, Clint Basinger was unpacking a few stray boxes in the living room, when out of nowhere at around midnight, he heard a voice echoing down the hallway from the other side of the house. “Good night,” the voice said. “It’s bedtime.”

Then, he heard the sound of locks clicking. “I couldn’t do anything with the doors, all the windows were armed, all the motion sensors turned on,” said Mr. Basinger, who had spent 15 years saving up to buy the three-bedroom, split-level house in Asheville, N.C. “I had no clue what to do, so I just stayed locked inside the house that night.”

Turns out, the home’s previous owner had installed a smart security system that he neglected to tell Mr. Basinger about. “It was really disconcerting, being in a new place and having no control over what was happening,” said Mr. Basinger, 36, the host of a YouTube channel for retro technology and video game reviews.

These days, smart technology can be found within virtually any quotidian object in a home: televisions, fridges, voice assistants, doorbells, coffee makers, thermostats, lights, alarm clocks, vacuums, toothbrushes and more. According to a 2022 report from the technology company Plume, households in the United States had an average of 20 internet-connected devices.

As our digital footprints in the home grow, the myriad apps and accounts required to control these devices also widens. All this automation creates more opportunities for people to lose access or power over aspects of the home, or, like in the case of Mr. Basinger, never gain access in the first place.

“We tell ourselves this story that our home is the thing that we can control — it’s private, it’s protected, it’s our space,” said Heather Suzanne Woods, a communication professor at Kansas State University and the author of a forthcoming book on smart homes.

But that feeling of control — even in ideal conditions, where the person is the original device owner and they have sole access to it with a password they made up — is often not much more than an illusion.

At best, when we can’t fully govern our devices, the complicated internet-of-things ecosystems we’ve set up in our private spaces are annoying, time-consuming or costly to deal with. At worst, when bad actors, such as an abusive ex-partner, are connected to the devices, they can become tools of abuse — allowing people with malicious intentions, who are not even physically in the home, to surveil, taunt or mentally torment those inside.

“In cases where people have separated from their partners and are no longer living together, it creates a situation where people can feel like they did all this work to get away from them, but just a click of a button can bring back that sense of helplessness,” said Lana Ramjit, the director of operations at Cornell University’s Clinic to End Tech Abuse. “It creates the sense that you’ll never be free from this person and that the abuse is coming from everywhere. It’s more than just the direct ways of showing control, it’s setting the coffee maker off suddenly, turning off the A.C. or flickering the lights.”

What happens when you can’t get control of the devices in your home? Is your home controlling you?

A Feature, Not a Bug

Eventually, Mr. Basinger got ahold of his real estate agent, who connected him to the previous owner, who finally “let me into my own house,” he said. The previous owner created a guest account for Mr. Basinger to access the system, but he still doesn’t have full administrator access. After calling the system’s manufacturer, Vivint, Mr. Basinger learned he had to install an entirely new system to have full control over it, because the current one would soon be phased out. Having gone through so much trouble with the setup already, the thought of getting another one didn’t sound very appealing to Mr. Basinger, so he decided to leave it as is. Now, he can control most aspects of his home (for example, what time it tells him to go to bed — a service that he’s opted out of altogether), but not all (he’s unable to change where the devices are in his home).

It has crossed Mr. Basinger’s mind that the previous owner, who remains the administrator of the security system, could change the settings or spy on him. “If he really wanted to, he could just login and see who’s coming and going. He could theoretically change my temperature; it’s got all the climate controls,” Mr. Basinger said. “I get a notification on my phone when a door opens, so I’m assuming if the previous owner doesn’t have that turned off, he still gets those notifications.” Luckily, it hasn’t been a problem yet.

On one of the first days in the fall of 2019, Aaron Barden came home to find that the temperature inside his house was at 78 degrees. “It was incredibly hot, and I was just wondering, ‘What’s going on?’” said Mr. Barden, 32, an engineer living in New Hope, Minn. “That’s when I realized there was already programming in the smart thermostat.”

Mr. Barden had moved into the house a few months prior and had noticed that there was a Honeywell

smart thermostat installed, but he didn't think much of it at the time. He later learned that the previous owner had a custom heating and cooling schedule programmed in the thermostat.

"I tried to get remote access to it, because I was thinking to myself, it'd be nice to be able to just remotely set my thermostat to whatever I want," Mr. Barden said. "Except I couldn't do that because the thermostat had a registration code, which was associated with the account of the previous homeowner."

Though it was a time sink, Mr. Barden eventually figured out how to cancel the schedule and manually change the temperature settings on the physical device to his own preferences — as one would with a regular, "unsmart" thermostat.

Mr. Barden reached out to Honeywell's customer service department, which asked him to fill out a form to undo the association between the thermostat and the previous owner's account. "But by the time I got to that point," he said, "I figured out how to just do all the programming locally and not have it connect to the internet. So I didn't really bother."

"If we have authorization from the former homeowner to deactivate their account, and correct documentation from the new homeowner for customer set up, it is an easy process," said David Porter, Vivint's senior vice president of customer experience, in an email statement. "Alignment with the buyer and seller plays a key role in this — we recommend home buyers discuss with their agent prior to closing to avoid equipment missing and delayed deactivation."

A spokesperson for Resideo, the company that designs and services Honeywell Home smart thermostats, said that it "offers secure support to help simplify the process of moving into a home with our smart solutions" and provided a link to instructions on how to delist thermostats. "As the security of our customers and their devices is of highest priority, we take several steps during the transition of devices to ensure we protect both users before transferring control of the device to a new account."

The ability for others to control smart devices is "fairly implicit in the current design of many smart homes. It's a feature, rather than a bug," Ms. Woods said.

"Full control over one's smart home is, at least in the present tense, an impossibility," she said. "Part of that is because the whole purpose of a smart device is to give up control to someone or something — whether that is a device, a platform, its code. Users delegate work, thinking or management to smart devices."

'I lived in my home like I was a prisoner'

And then the darker side of smart living can emerge, with every nook and cranny of our domestic spaces filled with gadgets and gizmos.

Lindsey Song, a co-chair of the New York Cyber Abuse Task Force and the deputy director of Courtroom Advocates Project at Sanctuary for Families, said she's observed an uptick in smart home devices being used in cases of domestic abuse.

"There's been a rollout of so many different technologies in the homes that are really beneficial, but also extremely invasive. We constantly see this utilized against survivors whose abuser has left the

home and yet the abuser is still connected to them in that way," said Ms. Song. "They're still able to access their devices, accounts and information."

Remotely turning up the heat on a smart thermostat on a searing hot summer day. Turning the lights off and on. Displaying daunting messages, such as "I'm watching you," on television screens. Playing offensive or triggering songs on smart speakers. These are among the dozens of cases of smart home abuse that Ms. Song has witnessed in her work. (Wirecutter has published a guide to protecting oneself from domestic abusers utilizing smart home devices.)

Ms. Ramjit, of the Clinic to End Tech Abuse, said that part of the difficulty in putting an end to this type of abuse comes from the fact that it's hard to prove, to a court or to the device manufacturer, that the device is being utilized by an abuser. "Usually, it's a shared account, and the platform or vendor has no way of differentiating who is using it," Ms. Ramjit said. "It looks like an authorized user, because it is."

The legal system hasn't entirely caught up with smart devices either. In New York State, courts can order the abuser "to refrain from remotely controlling any connected devices affecting the home, vehicle or property of the person protected by the order." But not all orders of protection account for that.

"I have yet to see an order of protection with that provision included," Ms. Song said. "It's a new addition to the law, and I think judges and advocates and litigants are not familiar with it, so it hasn't really been put into practice much at all."

Jennifer Friedman, the director of Bronx and Manhattan Legal Project & Policy at Sanctuary for Families, recalled a case of a woman who was a victim of domestic violence and had an order of protection that barred her ex from entering the home. But the man would manipulate the home's smart locks from afar, locking and unlocking the front door at different times. "While he was excluded from the home and not permitted to be there, he was still managing the household from this app, which was terrifying to her," said Ms. Friedman.

Shamima Ahmed, 40, was talking on the phone in her living room, when she noticed a blinking red light on the ceiling. It was a home security camera, one of several more she would discover, placed by her husband at the time. The court had placed an order of protection barring Ms. Ahmed's husband, who physically and mentally abused her, from entering the home, but the cameras were his way of surveilling her from afar.

She felt acutely aware that every move she made could be being tracked and that even when her abuser wasn't home and was legally required to stay away, he still had a presence. "I felt like I couldn't talk. I lived in my home like I was a prisoner," said Ms. Ahmed, a hair and makeup artist in Queens.

Now divorced, Ms. Ahmed moved into a new home of her own, but the fear and feeling of being watched persist. At first, "I couldn't sleep," Ms. Ahmed said. "I still get panicked sometimes, and it took a while, but I told myself, 'This is my house, this is my safe place.'"

Category

1. Crime-Justice-Terrorism-Corruption
2. Main
3. NWO-Deep State-Dictatorship-Tyrrany

4. Science-Tech-AI-Medical & Gen. Research

Date Created
02/22/2023