

USA: Thermostats, locks and lights: Digital tools of domestic abuse

By Nellie Bowles

NY Times (23.06.2018) – <https://nyti.ms/2KrQ52q>– The people who called into the help hotlines and domestic violence shelters said they felt as if they were going crazy.

One woman had turned on her air-conditioner, but said it then switched off without her touching it. Another said the code numbers of the digital lock at her front door changed every day and she could not figure out why. Still another told an abuse help line that she kept hearing the doorbell ring, but no one was there.

Their stories are part of a new pattern of behavior in domestic abuse cases tied to the rise of smart home technology. Internet-connected locks, speakers, thermostats, lights and cameras that have been marketed as the newest conveniences are now also being used as a means for harassment, monitoring, revenge and control.

In more than 30 interviews with The New York Times, domestic abuse victims, their lawyers, shelter workers and emergency responders described how the technology was becoming an alarming new tool. Abusers – using apps on their smartphones, which are connected to the internet-enabled devices – would

remotely control everyday objects in the home, sometimes to watch and listen, other times to scare or show power. Even after a partner had left the home, the devices often stayed and continued to be used to intimidate and confuse.

For victims and emergency responders, the experiences were often aggravated by a lack of knowledge about how smart technology works, how much power the other person had over the devices, how to legally deal with the behavior and how to make it stop.

“People have started to raise their hands in trainings and ask what to do about this,” Erica Olsen, director of the Safety Net Project at the National Network to End Domestic Violence, said of sessions she holds about technology and abuse. She said she was wary of discussing the misuse of emerging technologies because “we don’t want to introduce the idea to the world, but now that it’s become so prevalent, the cat’s out of the bag.”

Some of tech’s biggest companies make smart home products, such as Amazon with its Echo speaker and Alphabet’s Nest smart thermostat. The devices are typically positioned as helpful life companions, including when people are at work or on vacation and want to remotely supervise their homes.

Some connected device makers said they had not received reports of their products being used in abuse situations. The gadgets can be disabled through reset buttons and changing a home’s Wi-Fi password, but their makers said there was no catchall fix. Making it easy for people to switch who controls

the account of a smart home product can inadvertently also make access to the systems easier for criminal hackers.

No groups or individuals appear to be tracking the use of internet-connected devices in domestic abuse, because the technology is relatively new, though it is rapidly catching on. In 2017, 29 million homes in the United States had some smart technology, according to a report by McKinsey, which estimated that the number was growing by 31 percent a year.

Connected home devices have increasingly cropped up in domestic abuse cases over the past year, according to those working with victims of domestic violence. Those at help lines said more people were calling in the last 12 months about losing control of Wi-Fi-enabled doors, speakers, thermostats, lights and cameras. Lawyers also said they were wrangling with how to add language to restraining orders to cover smart home technology.

Muneerah Budhwani, who takes calls at the National Domestic Violence Hotline, said she started hearing stories about smart homes in abuse situations last winter. "Callers have said the abusers were monitoring and controlling them remotely through the smart home appliances and the smart home system," she said.

Graciela Rodriguez, who runs a 30-bed emergency shelter at the Center for Domestic Peace in San Rafael, Calif., said some people had recently come in with tales of "the crazy-making things" like thermostats suddenly kicking up to 100 degrees or smart speakers turning on blasting music.

“They feel like they’re losing control of their home,” she said. “After they spend a few days here, they realize they were being abused.”

Smart home technology can be easily harnessed for misuse for several reasons. Tools like connected in-home security cameras are relatively inexpensive – some retail for \$40 – and are straightforward to install. Usually, one person in a relationship takes charge of putting in the technology, knows how it works and has all the passwords. This gives that person the power to turn the technology against the other person.

Emergency responders said many victims of smart home-enabled abuse were women.

Connected home gadgets are largely installed by men, said Melissa Gregg, a research director at Intel working on the implications of smart home technology. Many women also do not have all the apps on their phones, said Jenny Kennedy, a postdoctoral research fellow at RMIT University in Melbourne, Australia, who is researching families that install smart home technology.

(One in three women and one in four men have been victims of physical violence or stalking by an intimate partner, according to a 2010 Centers for Disease Control report.)

The people who spoke to The Times about being harassed through

smart home gadgetry were all women, many from wealthy enclaves where this type of technology has taken off. They declined to publicly use their names, citing safety and because some were in the process of leaving their abusers. Their stories were corroborated by domestic violence workers and lawyers who handled their cases.

Each said the use of internet-connected devices by their abusers was invasive – one called it a form of “jungle warfare” because it was hard to know where the attacks were coming from. They also described it as an asymmetry of power because their partners had control over the technology – and by extension, over them.

One of the women, a doctor in Silicon Valley, said her husband, an engineer, “controls the thermostat. He controls the lights. He controls the music.” She said, “Abusive relationships are about power and control, and he uses technology.”

She said she did not know how all of the technology worked or exactly how to remove her husband from the accounts. But she said she dreamed about retaking the technology soon.

“I have a specific exit plan that I’m in the process of implementing, and one of my fantasies is to be able to say, ‘O.K. Google, play whatever music I want,’” she said. Her plan with the smart thermostat, she said, was to “pull it out of the wall.”

When a victim uninstalls the devices, this can escalate a conflict, experts said. "The abuser can see it's disabled, and that may trigger enhanced violence," said Jennifer Becker, a lawyer at Legal Momentum, a women's rights legal advocacy group.

Eva Galperin, director of cybersecurity for the Electronic Frontier Foundation, a digital rights group, said disabling the devices could also further cut off a victim. "They're not sure how their abuser is getting in and they're not necessarily able to figure it out because they don't know how the systems work," Ms. Galperin said. "What they do is they just turn everything off, and that just further isolates them."

Legal recourse may be limited. Abusers have learned to use smart home technology to further their power and control in ways that often fall outside existing criminal laws, Ms. Becker said. In some cases, she said, if an abuser circulates video taken by a connected indoor security camera, it could violate some states' revenge porn laws, which aim to stop a former partner from sharing intimate photographs and videos online.

Advocates are beginning to educate emergency responders that when people get restraining orders, they need to ask the judge to include all smart home device accounts known and unknown to victims. Many people do not know to ask about this yet, Ms. Becker said. But even if people get restraining orders, remotely changing the temperature in a house or suddenly turning on the TV or lights may not contravene a no-contact order, she said.

Several law enforcement officials said the technology was too new to have shown up in their cases, though they suspected the activity was occurring.

“I’m sure that it’s happening,” said Zach Perron, a captain in the police department in Palo Alto, Calif. “It makes complete sense knowing what I know about the psychology of domestic violence suspects. Domestic violence is largely about control – people think of physical violence but there’s emotional violence, too.”

Some people do not believe the use of smart home devices is a problem, said Ruth Patrick, who runs WomenSV, a domestic violence program in Silicon Valley. She said she had some clients who were put on psychiatric holds – a stay at a medical facility so mental health can be evaluated – after abuse involving home devices.

“If you tell the wrong person your husband knows your every move, and he knows what you’ve said in your bedroom, you can start to look crazy,” she said. “It’s so much easier to believe someone’s crazy than to believe all these things are happening.”

Asking everyone in a home to understand smart home technology is essential, researchers said.

“When we see new technology come out, people often think,

'Wow, my life is going to be a lot safer,'" said Katie Ray-Jones, chief executive of the National Domestic Violence Hotline. But "we often see the opposite with survivors of domestic violence."

.....

If you want to be regularly informed about different violations of human rights in the world, click here for a free subscription to our newsletters!

Also:

HRWF database of news and information on over 70 countries:<http://hrwf.eu/newsletters/womens-rights-gender-equality/>

List of hundreds of documented cases of believers of various faiths in 20 countries: <http://hrwf.eu/forb/forb-and-blasphemy-prisoners-list/>