'PrivacyMic': For a smart speaker that doesn't eavesdrop

9 June 2021, by Gabe Cherry

Credit: Pixabay/CC0 Public Domain

Microphones are perhaps the most common electronic sensor in the world, with an estimated 320 million listening for our commands in the world's smart speakers. The trouble is that they're capable of hearing everything else, too.

But now, a team of University of Michigan researchers has developed a system that can inform a smart home—or listen for the signal that would turn on a smart speaker—without eavesdropping on audible sound.

The key to the device, called PrivacyMic, is ultrasonic sound at frequencies above the range of human hearing. Running dishwashers, computer monitors, even finger snaps, all generate ultrasonic sounds, which have a frequency of 20 kilohertz or higher. We can't hear them—but dogs, cats and PrivacyMic can.

The system pieces together the ultrasonic information that's all around us to identify when its services are needed, and sense what's going on around it. Researchers have demonstrated that it can identify household and office activities with greater than 95% accuracy.

"There are a lot of situations where we want our home automation system or our smart speaker to understand what's going on in our home, but we don't necessarily want it listening to our conversations," said Alanson Sample, U-M associate professor of electrical engineering and computer science. "And what we've found is that you can have a system that understands what's going on and a hard guarantee that it will never record any audible information."

Ubiquitous computing + privacy

PrivacyMic can filter out audible information right on the device. That makes it more secure than encryption or other security measures that take steps to secure audio data after it's recorded or limit who has access to it. Those measures could all leave sensitive information vulnerable to hackers, but with PrivacyMic, the information simply doesn't exist.

While smart speakers are an obvious application, the research team envisions many others that, while less common, may be more important. In-home ultrasonic devices, for example, could monitor the homes of the elderly for signs that they need help, monitor lung function in respiratory patients or listen to clinical trial participants for sonic signatures that could reveal medication side effects or other problems.

"A conventional microphone placed in somebody's home for months at a time could give doctors richer information than they've ever had before, but patients just aren't willing to do that with today's technology," Sample said. "But an ultrasonic device could give doctors and medical schools unprecedented insight into what their patients' lives are really like in a way that the patients are much more likely to accept."

The idea behind PrivacyMic began when the team was classifying previously recorded audio. Looking at a visual graph of the data, they realized that audible sound was only a small piece of what was available.

"We realized that we were sitting on a lot of interesting information that was being ignored. We could actually get a picture of what was going on in a home or office without using any audio at all," said Yasha Iravantchi, a graduate student in electrical engineering and computer science and first author on a new paper on the research.

Listening for ultrasonic sound

Armed with this insight, a laptop and an ultrasonic microphone, the team then went to work capturing audio from tooth brushing, toilet flushing, vacuuming, running dishwashers, using computer monitors and hundreds of other common activities. They then compressed the ultrasonic signatures into smaller files that included key bits of information while stripping out noise within the range of human hearing—a bit like an ultrasonic MP3—and built a Raspberry Pi-based device to listen for them.

The device, which can be set to filter out speech or to strip out all audible content, accurately identified common activities more than 95% of the time. The team also conducted a trial where study participants listened to the audio collected by the device and found that not a single participant could make out human speech.

While the device is a proof of concept at this stage, Sample says that implementing similar technology in a device like a smart speaker would require only minor modifications—software that listens for ultrasonic sound and a microphone capable of picking it up, which are inexpensive and readily available. While such a device is likely several years off, the team has applied for patent protection through the U-M Office of Technology Transfer.

"Smart technology today is an all-or-nothing proposition. You can either have nothing or you can have a device that's capable of constant audio recording," Sample said. "PrivacyMic offers another layer of privacy—you can interact with your device using audio if you choose or you can have another setting where the device can glean information without picking up audio."

The paper is titled "PrivacyMic: Utilizing Inaudible Frequencies for Privacy Preserving Daily Activity Recognition." The researchers presented it May 12 at the ACM CHI Virtual Conference on Human Factors in Computing Systems.

More information: Yasha Iravantchi et al, PrivacyMic: Utilizing Inaudible Frequencies for Privacy Preserving Daily Activity Recognition, *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (2021). DOI: 10.1145/3411764.3445169

Provided by University of Michigan