TECHNOLOGY

Everything You Do Is Being Recorded

Is there any way of fighting back?

By Ross Andersen

Illustration by The Atlantic. Source: Getty.

MAY 18, 2026 SHARE AS GIFT DISCUSS 75 REMOVE

Anthony "Bingy" Arillotta waited years to become a made man in the Genovese crime family, and when at last the call came in August 2003, he followed directions to the letter. According to sworn testimony, Arillotta was summoned to a steak house in the Bronx, where he was made to hand over his cellphone, beeper, and jewelry before being driven to an apartment building. When he got there, he was taken to a small bathroom and strip-searched for electronic devices. For his big meeting with the boss, he was given a bathrobe to wear.

Until recently, only spies and criminals had to worry this obsessively about their private statements being picked up by electronic equipment. But soon, the average

person might need to deploy surveillance countermeasures. The next time you conduct a delicate bit of office diplomacy or share a romantic or financial secret with a friend over drinks, a sensor built into someone's glasses, necklace, or lapel pin might be watching you and listening.

In March, the tech start-up Deveillance announced the development of Spectre I, a hockey-puck-shaped device that purports to prevent others from recording you (no strip search required). The company was founded by Aida Baradari, a recent college graduate who was worried by the surge in people wearing AI-enabled recorders. These wearables can be used as a silent notetaker, a personal assistant, or even a therapist of sorts. That technology isn't yet mainstream, but it may be soon. Apple—the company with the largest personal-tech ecosystem in the world—is rumored to be developing an AI pin or pendant that would serve as an iPhone's constant eyes and ears; many other products of this type are on the way. AI accessories could one day be as widespread as AirPods.

New surveillance technologies tend to breed new countermeasures, which lead, in turn, to more sophisticated surveillance. During the Second World War, after Germany operationalized radar, the Royal Air Force began dropping thin strips of metallized paper cut to a specific size that resonated with the radar, swamping German screens with phantom echoes that were indistinguishable from real aircraft. Some historians have argued that the ensuing radar arms race was more consequential to the war's outcome than the Manhattan Project.

For decades, crude jammers have been sold to people who hope to avoid being recorded. Early versions blasted loud, unpleasant white noise to conceal voices. More recently, companies have made models that emit a steady stream of ultrasonic sound at inaudible frequencies, exploiting a quirk of microphone hardware that converts those high frequencies into noise. In 2020, a team at the University of Chicago led by Yuxin Chen reported that it had mounted 23 ultrasonic transducers on a single bracelet, such that jamming signals could be sent in all directions instead of being focused on a single target.

Read: The most reviled tech CEO in New York confronts his haters

But even high-tech jammers have a hard time fending off today's AI wearables. The most advanced pins, pendants, and glasses use speech-recovery algorithms to strip away unwanted noise, whether it originates from everyday sources—such as the clinking of glasses in a crowded bar—or from an ultrasonic jammer. This task the

algorithms perform is quite difficult: In that crowded bar, a microphone on a person's lapel will intercept sound vibrations from many different sources at once. It will pick up a bartender calling out a drink order, music emanating from a speaker, bursts of laughter coming from nearby tables—and all of these sounds ricochet off of walls and other objects, creating yet more noise. The human body solves this "cocktail party problem" without us noticing: Our ears serve as dual microphones, and our brain can use the timing and intensity differences between them, along with layered processing in the auditory cortex, to isolate the voice of a person who is sitting across from us.

DeLiang Wang, a computer scientist at Ohio State University, has spent decades training neural networks to accomplish that same goal, for the purpose of improving hearing aids. By feeding the networks hundreds of hours of recorded human voices, he has taught them to recognize the frequencies and rhythms of speech. The models build an internal representation of "speech-ness," and when they encounter a noisy recording, they focus on the parts that match the patterns they have learned and then suppress everything else. The most advanced technologies can now infer missing syllables in the way that a reader fills in a redacted word from context, allowing them to reconstruct speech that wasn't cleanly captured in the first place.

Big tech companies are trying to do this too. Microsoft has been running an annual Deep Noise Suppression Challenge since 2020 to advance the field. (Their in-house team is trying to make Teams meetings less excruciating.) Other companies are working on noise cancellation for cellphone calls and podcast software. This sort of research is meant to improve the lives of normal users of technology—assuming that we podcast listeners count as normal—but every advance in de-noising can also be used to help an AI assistant recover speech from a jammed recording.

Defeating these algorithms may require a different countersurveillance approach altogether. Finn Brunton, a historian at UC Davis and the co-author of *Obfuscation: A User's Guide for Privacy and Protest*, told me that one of the best ways is to identify the data that a device is trying to collect, and then supply it with a junk version. The Berlin-based artist Adam Harvey used this strategy when he developed makeup and clothing that frustrate facial-recognition algorithms. Daniel Howe and Helen Nissenbaum did something similar with a browser plug-in called TrackMeNot: Rather than concealing a user's Google searches, the extension continually runs its own randomized decoy queries in the background, so that whatever a user actually searched for becomes lost in a sea of false leads.

People have tried this technique in the realm of audio too. Woodrow Hartzog, a law

professor at Boston University who studies privacy and surveillance, told me that early in his legal career, he worked with defense attorneys who worried that their jailhouse conversations with clients would be recorded. To fight back, they played "babble tapes"—audio files layered with 40 tracks of voices in different accents—in the background.

In 2023, a team led by Ming Gao, now a researcher at Nanjing University, used human voices to defeat speech-recovery algorithms in a different way. Its jammer, called MicFrozen, is worn by a speaker who doesn't want to be recorded. It listens as they talk and then generates a real-time stream of ultrasonic "anti-speech" tuned to the speaker's voice, much like the noise-cancellation technology in your headphones. The device then sends out another layer of counterfeit speech-shaped sound to mislead any algorithm that tries to reconstruct what was lost.

Baradari, whose company is working on the Spectre I device, wouldn't tell me exactly how her jammer's signals work, but she said that they, too, resemble speech. The launch video for Spectre I claims that the device will also be able to detect the presence of nearby microphones. When I asked Baradari how it will do that, she clarified that her team is still "working on that part right now."

However effective Spectre I turns out to be, it won't be the end of the recording arms race. More capable AI models may eventually deploy some new listening tricks of their own. They may bypass recorded audio altogether. In Stanley Kubrick's *2001: A Space Odyssey*, when two astronauts retreat to a soundproofed pod to discuss disconnecting HAL 9000, the ship's computer simply reads their lips through the porthole. A wearable powered by a model that's been trained on enough conversation footage could, in principle, do the same. In theory, it could also stare at a glass of water between two people and recover their speech from vibrations on the liquid's surface.

AI wearables may always have an edge over countermeasures. After all, they're using a technology that is a product of the entire speech-processing industry, which takes in billions of dollars in investments—not just for AI assistants but also for hearing aids, smart speakers, and teleconferencing tools. Meanwhile, only a few academics and small companies are defending us from these technologies. "The thing about cat-and-mouse games is that we know how they usually end up for the mouse," Hartzog said. "And in this case, the cat includes some of the most powerful corporations to ever exist."

The Mafia knows what it's like to be a mouse. By the time Arillotta, the aspiring made man, was told to put on the bathrobe, criminal organizations had been engaged in surveillance arms races of their own for decades. After law enforcement started bugging their phones, bosses would conduct business in person. Sometimes, they'd use a safe house or a vehicle, but those could be bugged, too, and so sensitive information might have been communicated only during a walk-and-talk. Eventually, crime families turned to burner phones, and then devices with encryption. But here, again, they fell prey to the cat.

In 2018, the FBI began secretly running Anom, its own encrypted-phone company. Through informants, it sold 12,000 devices with a special Anom messaging app. Members of Mafia families, motorcycle gangs, and other criminal organizations treated the phones as a status symbol, and used them to negotiate drug deals, launder money, and participate in all manner of other illegal activity. But the security that they offered was a ruse: Every message that they sent was being intercepted by the feds.

View Discussion 75

ABOUT THE AUTHOR

Ross Andersen

Follow

Ross Andersen is a staff writer at *The Atlantic*. He was previously the magazine's deputy editor. As a writer for the magazine, he has reported from Greenland, Russia, India, Pakistan, China, South Korea, and Japan. He is also the author of *The Long Search*, forthcoming from Random House.