



The Information shared this article with you. Don't miss out on the next one. Subscribe to The Information.

Subscribe Now →

**EXCLUSIVE**    AMAZON    E-COMMERCE

# Amazon Echo and the Hot Tub Murder

By Tom Dotan and Reed Albergotti Dec 27, 2016 7:01 AM PST

**Subscribe now**

**B**e careful what you say around your Amazon Echo. Your words may be recorded and used against you in court.

In what may be the first case of its kind, police investigating a murder in Bentonville, Arkansas, issued a warrant to Amazon.com to turn over audio and other records from an Echo. The device in question belongs to James Andrew Bates, who was charged earlier this year with first-degree murder. The victim, Victor Collins, **was found dead in Mr. Bates' hot tub** one Sunday morning in November of last year.

## THE TAKEAWAY

**Internet of Things devices that are always listening are emerging as a new tool for police, raising the prospect of more**

battles between tech companies and law enforcement. In this case, Arkansas detectives got a search warrant for an Amazon Echo in the house where a man was murdered late last year.

According to court records, Amazon twice declined to hand over information the Echo transmitted to its servers. The company did hand over Mr. Bates' account information and purchase history. Police also said they took the device and extracted data off it, the records show. Amazon did not respond to questions about the case or how it responded to the search warrant.

Mr. Bates pleaded not guilty in April and is out on bail. The case is due to go to trial in early 2017, according to Mr. Bates' defense attorney. Police referred questions to the prosecutor's office, which didn't respond to a request for comment.

This murder investigation in a 40,000-person town in Arkansas, miles away from Silicon Valley or Seattle, offers a glimpse at the kinds of investigations that will increasingly become commonplace, lawyers specializing in electronic privacy say. In one sense, the episode has echoes of Apple's showdown with the FBI over unlocking an iPhone belonging to the alleged San Bernardino shooter. But the "always on" Internet of Things devices—which record and remotely store snippets of audio—present a new wrinkle as fodder for criminal investigations.

It's a relevant issue for a growing number of people. The Echo was a widely popular holiday gift this year; Amazon sold out of the full-sized model and on Christmas Day the companion app shot to the top five most downloaded free apps on the iTunes store, above Facebook and Instagram.

In this case, Mr. Bates had several IoT devices in his home, according to police records filed with the court. These included a Nest Thermostat, a Honeywell Alarm System, a wireless weather monitoring system and an unopened remote-activated lighting device—as well as the Echo.



One big question is how much data could potentially be available from the device. An Echo is equipped with seven microphones that are always “on,” listening for a person to utter a “wake word” like “Alexa” before perking up. At that point, it records a person’s commands—but only records while the device’s blue light is on, according to a person close to Amazon. That data is sent to Amazon’s cloud servers where it can carry out tasks like telling someone the weather, playing music or setting an alarm.

That would limit how much data could be captured. But as most owners probably have experienced, the microphones can often be triggered inadvertently. And those errant recordings, like ambient sound or partial conversations, are sent to Amazon’s servers just like any other. A look through the user history in an Alexa app often reveals a trove of conversation snippets that the device picked up and is stored remotely; people have to delete those audio clips manually.

"The interesting thing in a murder trial would be if there was this 'false fire' [accidental recording] and audio snippets were recorded in the process," said Todd Mozer, CEO of Sensory, which builds so-called "embedded speech recognition" in products made by companies like Samsung, Amazon and Motorola.

Mr. Bates’ defense attorney, Kimberly Weber, said in an interview it was alarming that police are now issuing warrants for an “always on” device. “You have an expectation of privacy in your home, and I have a big problem that law enforcement can use the technology that advances our quality of life against us,” Ms. Weber said.

Mr. Mozer said that even more interesting than analyzing Alexa data to solve a murder case is a scenario where a government agency went to a company like Google and asked them to remotely configure a voice recognition device to constantly record a suspected terrorist. "Is the plumbing in place to allow the device to do that? I suspect there is," he said.

## **IOT Skepticism**

Some are skeptical about the potential of IoT devices to help police investigations. In a Feb. 5 letter to Harvard professor and privacy advocate Jonathan Zittrain, who authored a paper about how IoT devices can be used for surveillance, Manhattan District Attorney Cyrus Vance argued that the Internet of Things won't end up being as useful as cell phones in criminal investigations. "Even if evidence collection through IoT can be done efficiently," he said, "People with something to hide can (and will) choose to avoid IoT."

It's unclear whether a tech company would be compelled to turn over customer data from an IoT device, said Ian Ballon, an Internet litigator at Greenberg Traurig. Most case law revolves around cell phone towers and location data, rather than Internet of Things devices—and much of it relates to the Electronic Communications and Privacy Act, which was crafted in the 1980s.

Moreover, there is a discrepancy in data collection rules between civil and criminal cases. As current law stands, in a civil case, someone can only get information about what time someone communicated with a device or for how long, but wouldn't be able to get "content data" like an audio recording. But it theoretically could in a criminal case, Mr. Ballon said.

As for Mr. Bates, court records suggest the device prosecutors got more from wasn't the Alexa but the home's smart water meter. It showed that someone used 140 gallons of water between 1 a.m. and 3 a.m. at Mr. Bates' house, a much heavier than usual amount. Prosecutors allege that was a result of Mr. Bates using a garden hose to spray down the back patio area from the blood. Ms. Weber is disputing the accuracy of the smart meter readings. And, in a decidedly non-digital strategy, she says the water outside the tub couldn't have come from a garden hose. Mr. Bates had a salt water tub, and she says all the water on the outside of the tub had salt residue.



6 TOTAL COMMENTS

Danny Sullivan, James Bishop and 4 others commented on this article.

READ COMMENTS FROM TOP TECH AND INDUSTRY LEADERS

ri  
Dropbox



**Joe Lonsdale**  
Founding Partner, Eight


View Joe's' profile →



**Chamath Palihapitiya**  
Founder & Managing Partner, SocialCapital



**Tina Sha**  
CEO, Bran

**Login** or **Subscribe** to follow the discussions happening  
here and real-time in our  **Slack** Community.



# Recent Articles



ASIA GOOGLE E-COMMERCE



MEDIA ENTERTAINMENT



AMAZON E-COMMERCE

## The Reality Behind Voice Shopping Hype

By Priya Anand



AMAZON E-COMMERCE

## Behind Some Low Amazon Prices: Stolen Goods

By Reed Albergotti

