The Walls Have Ears: Warrant Granted For Amazon Echo Home Data, Setting Precedent

by Tyler Durden

Submitted by Alice Salles via TheAntiMedia.org,

Technology has, for the better part of the last decade, changed our lives in significant and groundbreaking ways. **But as technology continues to make great strides, helping us change the way we do business and live our lives, it is also employed by bureaucrats looking to keep an eye on everyone.**

Thanks to Edward Snowden and others before him, like former U.S. National Security Agency (NSA) intelligence official William Binney, we now know U.S. officials make use of secret courts to gain access to phone records — ignoring due process and, of course, the 4th Amendment to the U.S. constitution. But even though the NSA revelations were widely discussed and privacy advocates have continued to press legislators and officials to justify the illegality of their actions, things seem to have only gotten worse — at least as far as official government policy is concerned.

Instead of reforming the system to make sure officials observe the constitution, laws have been passed to increase the government's access to technologies used widely by Americans and visitors. The result? The widespread normalization of government spying.

Instead of sweeping outrage, many Americans continue to feel that being spied upon is part of their everyday lives — and that instead of fighting it, they should embrace it as a means to protect the country from external forces.

To nearly half of the population, recent news about a court order regarding a private Amazon Echo may not seem as shocking as it should.

Warrant Issued for Amazon Echo Device, Setting a Precedent

A case involving a murder in Arkansas just helped the public learn that companies like Amazon often retain recordings of people's conversations through devices like Amazon Echo — and that these recordings are stored in servers that may later be subject to law enforcement investigations. Depending on how the case shapes up, it could set a legal precedent that would open up government access to similar smart devices, and even force companies to keep these recordings in storage for future investigations.

The first warrant naming this specific device was tied to a Bentonville, Arkansas, murder that happened in November 2015. The official document asked the company to release "*any recordings between*

November 21 and November 22, 2015." **The Amazon Echo device in question belongs to James Andrew Bates, the suspect facing a first-degree murder charge associated with the death of his friend, Victor Collins. Collins was allegedly strangled and drowned in Bates' hot tub.**

> In the search warrant, police wrote that the "*records … retained by Amazon.com … are evidence related to the case under investigation*." Nevertheless, Amazon did not release any data. Instead, the company provided investigators with the suspect's account details, which include past purchases. Despite Amazon's decision not to cooperate unless "*a valid and binding legal demand properly [is] served*," officials may still be able to recover information from the device's speakers without the company's help.

> ***"Even without Amazon's help," CNET* reported*, "police may be able to crack into the Echo"* by tapping *"into the hardware on the smart speakers, which could 'potentially include time stamps, audio files or other data.'"***

Other smart devices covered by this warrant included Collins and Bates' phones, a wireless weather monitoring system, a WeMo device used for lighting, a Nest thermostat, and a Honeywell alarm system.

If this case serves as an example of anything, it is that your privacy is not protected, even if companies like Amazon refuse to cooperate with law enforcement under certain circumstances. With or without a warrant, officials will continue to use similar devices against their owners.

Regardless of what law enforcement finds on Bates' Amazon Echo, evidence gathered by smart devices will continue to be employed by government officials. The only way to protect yourself is to follow good online security practices, which will help to protect your data from future breaches.

Could your high-tech gadgets send you to jail?

The Amazon Echo hands-free voice-activated speaker could figure in an Arkansas murder investigation — and remind people that their internet-connected gadgets constantly collect information about their private lives. TNS .
By Scott Canon

Feel like no one ever really listens to you?

Your gadgets do. That may not always be a good thing.

Most recently, an Arkansas death investigation highlighted how the magic of Amazon's Echo device — its ability to act on your voice commands — means it might have overheard conversations critical to a murder investigation.

"Only naive people will put a government listening device in their own homes"

That case could ultimately lasso Amazon's cloud of remote computer storage into court fights. The results hold implications for the many ways technology's romp toward ubiquity poses a growing threat to privacy.

It also acts as a reminder that buying a so-called smart speaker such as the Echo — or its chief competitor, Google Home — is like plugging Big Brother into your living room.

Those computerized sound systems are just the latest listeners to the party.

Your smartphone already mines mountains of personalized data (note how many apps seek access to your contacts, location, camera and microphone). The resulting cache of information creates a defining dilemma of the Digital Age.

The more bits about your life you share with your gadgets, the better help you'll get from Siri, from your Fitbit, from your Google searches.

Yet in maximizing that functionality, you leave untold digital bread crumbs that could someday be used against you by an angry former lover, by some ransom-seeking East European hacker, by the cops.

"There's always a gap between when people lose their privacy and when they *realize* they've lost it," said Jay Stanley, a technology policy analyst for the American Civil Liberties Union. "When all kinds of exciting new services are being thrown at you, you lose track."

Better listeners

The latest techno turn comes with galloping advances in voice recognition. In the mid-1990s, the best voice recognition software suffered error rates of about 95 percent. This fall, a team of Microsoft engineers published a paper documenting that robots hear better than you do. The researchers wrote that "our automated system establishes a new state-of-the-art, and edges past the human benchmark."

Whether you're calling out "Alexa" to your Amazon Echo, "Hey Siri" to your iPhone, "Hey Cortana" to your Microsoft desktop or "OK Google" to your Android device, you've summoned help not just from a particular gadget but from the corporate computer banks scattered around the globe.

Those commands "all involve a computer near you, listening to everything all the time, and looking for the magic activation phrase," said Dan Wallach, a computer science professor at Rice University. "After that, they record everything they hear and send it to the cloud for recognition. It's much easier to do high quality voice recognition in the cloud, where they've got sophisticated machine learning models."

That means the scraps from your life get stored in computer servers connected to the internet. That puts them out of your control. Court cases have long held — although groups such as the ACLU contend the law needs updating — that police often don't need warrants to access the files from a third party like they would to search your home.

Anybody with a Gmail account can get a quick taste of how just one corporation can store a fairly intimate portrait of a user. It can map out your location over time — how many times you went to church, or to a bar. It catalogs Web searches, the YouTube videos you watched, the music you listen to.

Users signed into that myactivity.google.com site will also find what the company calls "voice and audio." It's mostly clips a few seconds long. The majority come from deliberate "OK Google" voice queries to a phone seeking the score of a ballgame or ingredients to a recipe.

But others are random bits of sound from the user's life, where the phone misheard random syllables as a call to attention.

"If the police could order Google or one of these other vendors to *deliberately* make recordings and upload them, on demand, then you've got an audio bug — a surveillance device — sitting in your pocket or on your desk," Wallach said.

Electronic witness

In the Arkansas case, the cops didn't trigger Echo to listen. But they want to know what it might have picked up.

They showed up after a resident, James A. Bates, called 911 and said that he'd awakened after a night of drinking and found the body of his friend Victor Collins floating in the backyard hot tub. Police ultimately launched a homicide investigation and suspected some clues might have been inadvertently gathered by the "Internet of things" — gadgets such as a Nest smart thermostat, a smart water meter, a Honeywell alarm system and Bates' Amazon Echo.

The Information reported this week that police pressed Amazon for help. They served a warrant to the online seller.

"The Amazon Echo device is constantly listening for the 'wake' command of 'Alexa' or 'Amazon,' and records any command, inquiry, or verbal gesture given after that point, or possibly at all times without the 'wake word' being issued, which is uploaded to Amazon.com's servers at a remote location," an affidavit with the warrant reads. "It is believed that these records are retained by Amazon.com and that they are evidence related to the case under investigation."

So far, Amazon has refused to comply with the warrant.

"Amazon will not release customer information without a valid and binding legal demand properly served on us," the company said in a statement. "Amazon objects to overbroad or otherwise inappropriate demands as a matter of course."

Commands to the Echo are recorded in the device whenever it hears the words "Amazon" or "Alexa," although they can be deleted later. The company says the device does not listen to other conversations, but any Echo owner has experienced random phrases that turn on the blue light to indicate it's listening for instructions.

Law enforcement has increasingly leaned on digital archives to solve cases and arm prosecutors with evidence. Cellphone records not only log calls, they can pinpoint someone's location at a specific time even when the device sits unused in a pocket or purse.

A computer forensic unit at the Kansas City FBI office increasingly looks to digital records in criminal investigations, said spokeswoman Bridget Patton.

"We live in a digital world and that all can come into play in conducting an investigation," she said. "It's more important all the time. We obtain that digital evidence lawfully."

Wired to hear

The Arkansas Echo example is just one of the myriad ways internet-reliant devices collect snippets of our lives. The paranoid and privacy-sensitive among us can tweak the settings on their gadgets to limit that — at the expense of utility. A smartphone can't steer you to the closest gas station, for instance, unless you let it know where you are.

"If you have not taken the time to check all your settings, you're going to be tracked," said Paul Stephens, the director of policy and advocacy for the Privacy Rights Clearinghouse.

Phone apps often require access to various functions on users' devices. Stephens noted that some flashlight apps ask for access to cameras and microphones "when there's no way they need that just to turn on that light."

Yet app makers are driven to mine data they can sell to marketers. He suggests simply going to a website of an airline or Facebook rather than downloading an app. It might be more cumbersome, but the move protects privacy.

The mere act of carrying a smartphone or outfitting your house with smart appliances can make people vulnerable to hackers. Google Glass, the failed project that perched an internet screen on users' noses, was hacked to turn on its camera surreptitiously. That sort of vulnerability to online intruders is why so many people tape over their laptop's camera.

"The situation is inherently double-edged," said Alan Sherman, a professor of computer science at the University of Maryland, Baltimore County. "There could be a legitimate reason why your toaster oven is connected to the internet. The manufacturer can track its performance and update the software to improve performance."

But, he wonders, is it a worthwhile trade-off to get the perfect frozen pizza in return for more eyes peeking into your kitchen?

The question may be increasingly moot. The to-and-fro of information is increasingly built into more devices, from our cars to our home music systems. Rapid improvements in voice recognition drive the latest wave.

"People are saying these things are very cool and a little creepy, but mostly cool," said Jim Barry, a spokesman for the Consumer Technology Association.

The Echo, he said, only accelerates the trend. Backed by the biggest seller of consumer goods in the world, Amazon’s gadget works well enough that people who resisted voice-activated devices are now warming to them.

“It’s got to be easy to use and do something you do frequently, like listen to music,” Barry said. “You’re only going to see more of this stuff.”