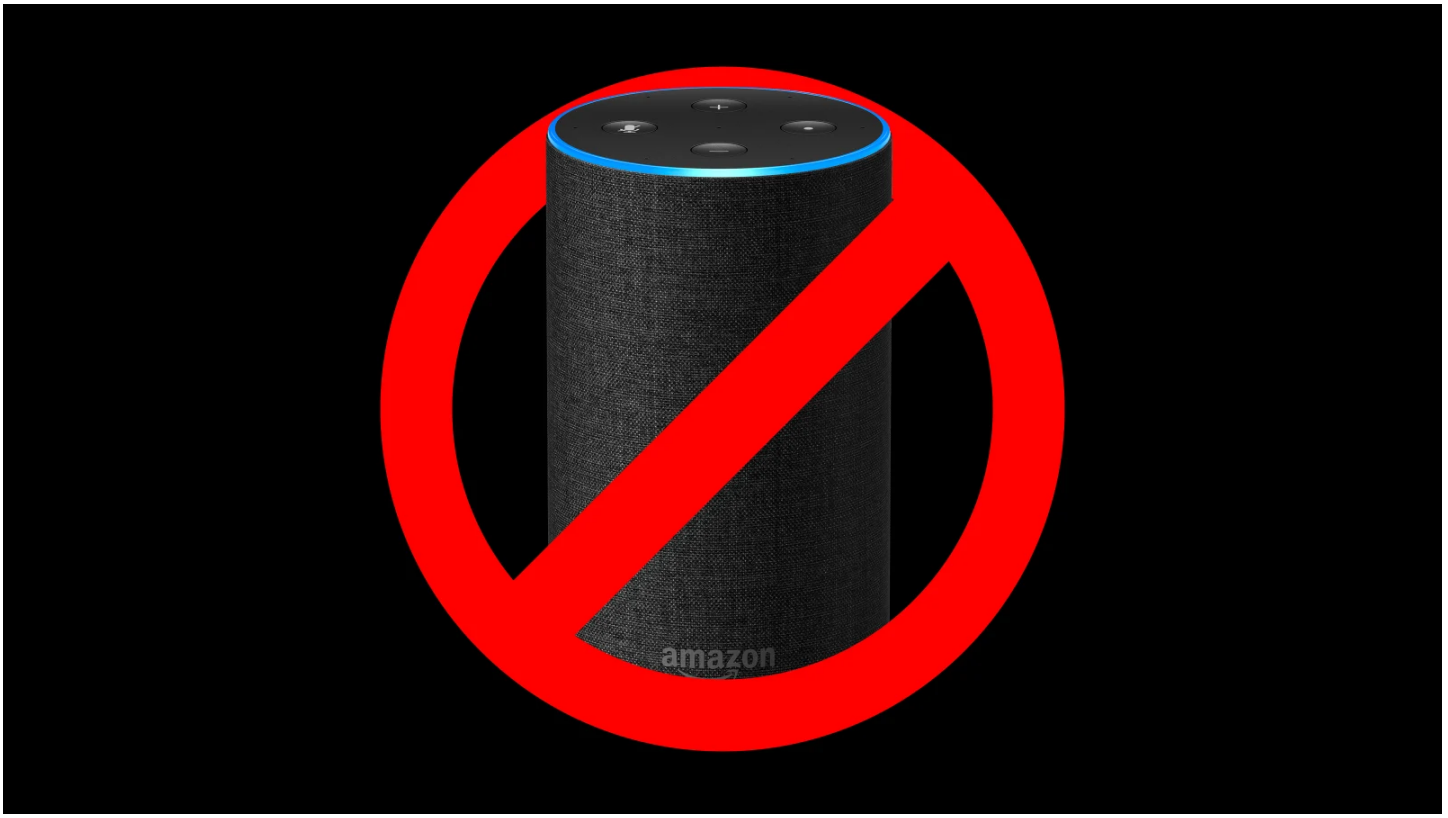
Don't Buy Anyone an Echo

Adam Clark Estes
12/05/17 10:28AM • Filed to: GRINCH WEEK



Amazon/Gizmodo

Three years ago, we said the Echo was "the most innovative device Amazon's made in years." That's still true. But you shouldn't buy one. You shouldn't buy one for your family. You definitely should not buy one for your friends. In fact, ignore any praise we've ever heaped onto smart speakers and voice-controlled assistants. They're bad!

What's challenging about this holiday season is that the futuristic gadgets are just so damn easy to buy. We've also given glowing reviews to several smart speakers and especially the Google Home devices. They're so pretty! Right now, smart speakers are cheaper than ever, too. Both Amazon and Google have slashed $20 off the price of their cheapest smart speakers, the Echo Dot and the Home Mini. That's $30 for gift

one of these!" If you really want to impress them, you can get the full-sized Amazon Echo or Google Home for $80 a piece—a discount of $20 and $50, respectively. Such savings!

Let me make this point dreadfully clear, though: Your family members do not need an Amazon Echo or a Google Home or an Apple HomePod or whatever that one smart speaker that uses Cortana is called. And you don't either. You only want one because every single gadget-slinger on the planet is marketing them to you as an all-new, life-changing device that could turn your kitchen into a futuristic voice-controlled paradise. You probably think that having an always-on microphone in your home is fine, and furthermore, tech companies only record and store snippets of your most intimate conversations. No big deal, you tell yourself.

Actually, it is a big deal. The newfound privacy conundrum presented by installing a device that can literally listen to everything you're saying represents a chilling new development in the age of internet-connected things. By buying a smart speaker, you're effectively paying money to let a huge tech company surveil you. And I don't mean to sound overly cynical about this, either. Amazon, Google, Apple, and others say that their devices aren't spying on unsuspecting families. The only problem is that these gadgets are both hackable and prone to bugs.

Before getting into the truly scary stuff, though, let's talk a little bit about utility. Any internet-connected thing that you bring into your home should make your life easier. Philips Hue bulbs, for instance, let you dim the lights in an app. Easy! A Nest thermostat learns your habits so you don't have to turn up the heat as often. Cool! An Amazon Echo or a Google Home, well, they talk to you, and if you're lucky, you might

be able to figure out how to talk back in the right way and do random things around the house. Huh?

You don't need an artificially intelligent robot to tell you about the weather every day. Just look outside or watch the local news or even look at your phone. You already do one or all of these things, so just keep it up. Same goes for turning on the lights. Use the switch. It works really well! A light switch also doesn't keep track of everything you're doing and send the data to Amazon or Google or Apple. What happens between you and the switch stays with you and the switch.

Which brings us back to security and surveillance. I'm not here to be Tin Foil Hat Man and convince you that companies like Amazon are spying on your every move and compiling data sets based on your activity so that they can more effectively serve you ads or sell you products. I am here to say that smart speakers like the Echo do contain microphones that are always on, and every time you say something to the speaker, it sends data back to the server farm. (By the way: If you enabled an always-listening assistant on your smartphone, now's a good time to consider the implications.) For now, the companies that sell smart speakers say that those microphones only send recordings to the servers when you use the wake word. The same companies are less explicit about what they're doing with all that data. They're also vague about whether they might share voice recordings with developers in the future. Amazon, at least, seems open to the idea.

We do know that Amazon will hand over your Echo data if the gadget becomes involved in a homicide investigation. That very thing happened earlier this year, and while Amazon had previously refused to hand over customer data, the company didn't argue with a subpoena in a murder case. It remains unclear how government agencies like the FBI, CIA, and NSA are treating smart speakers, too. The FBI, for one, would neither confirm nor deny wiretapping Amazon Echo devices when Gizmodo asked the agency about it last year.

Sinister ambitions of governments and multinational corporations aside, you should also worry about the threat of bugs and hackers going after smart speakers. Anything that's connected to the internet is potentially vulnerable to intrusions, but as a new category of devices, smart speakers are simply untested in the security arena. We haven't yet experienced a major hack of smart speakers, although there's plenty of evidence to suggest that they're hardly bulletproof. Not long after its launch, the Google Home Mini experienced a bug that led to the device recording everything happening in a technology reporter's house for dozens of hours. You can chalk that up to a very bad screw up on Google's part, but it's a tear in the fabric of trust that should encase these kinds of gadgets.

Hackers pretty much set that fabric on fire. A few months ago, *Wired* reported that a hacker successfully installed malware on an Amazon Echo and turned it into an always-on wiretap. The malware let the hacker stream all audio from the Echo to a remote server, which is some serious badass spy shit when you really think about it. This particular exploit only worked on devices made before 2017 and required the hacker to have physical access to the Echo. Nevertheless, it's sort of the worst possible scenario for anyone who's worried about having an always-on microphone in their home.

This is all to say that there are risks involved with owning a smart speaker. It's not as risky as, say, running a meth lab out of your basement. But keeping an internet-connected microphone in your kitchen is certainly more trouble than owning a simple Bluetooth speaker that just plays music. You might be comfortable taking that risk for yourself. Think long and hard about buying an Amazon Echo or a Google Home for your friends and family. They might not like it. In my opinion, they shouldn't.

Welcome to Grinch Week, a series in which we tell you what gifts not to buy this holiday season.

SHARE THIS STORY

GET OUR NEWSLETTER

Subscribe

MORE FROM GIZMODO

- **Amazon Agrees to Hand Over Data in Echo Murder Case**
- **It's Hard Not to Love the Google Home Mini**
- **The FBI Can Neither Confirm Nor Deny Wiretapping Your Amazon Echo**

ABOUT THE AUTHOR

Adam Clark Estes

Senior editor at Gizmodo.

Email Twitter Posts Keys

DISCUSSION

Staff (3) Community (410) Pending

Sort by: Popular

Reply

tobeistobex > Adam Clark Estes
12/05/17 10:42am

341

Can't these arguments be made about every phone and most apps also?

Reply | 37 replies

Adam Clark Estes > tobeistobex
12/05/17 11:26am

72

Many devices have microphones, and everything can be hacked. The question is:

Show all 410 replies

You May Like



Model Known As "Giraffe Woman" Takes Her Rings Off After Five Years

Post Fun

School Expels Teen Over Outfit, Regrets It When They See Who Dad Is

Top 5

Almost Nobody Aces This 1970s Car Quiz - Can You?

Autoversed.com

The 25 Greatest Cars America Has Ever Produced

DriveZing

This Is The Smartest Dog Breed According To Veterinarians

Science101

Prince Charles Made a Horrid Comment After Harry's Birth that Sparked Rumors and Brok...

SocialGazette