Amazon sent 1,700 Alexa voice recordings to the wrong user following data request

theverge.com/2018/12/20/18150531/amazon-alexa-voice-recordings-wrong-user-gdpr-privacy-ai

Nick Statt
December 19, 2018*Photo by Dan Seifert / The Verge*

Amazon's Alexa is among the most ubiquitous personal voice assistants on the planet, and it also happens to live inside the living rooms and bedrooms of millions of Alexa device owners around the world. That gives Amazon the responsibility of being a proper steward of the data it collects when we ask Alexa a question and or engage in back-and-forth conversations with the software.

Unfortunately, a case from Germany has highlighted the potential pitfalls involved with using such a product, when Amazon accidentally sent a man 1,700 Alexa voice recordings of another user by mistake, according to German magazine *c't*.

Following the passage of the European Union's General Data Protection Regulation, or GDPR, any EU resident may demand a company send them the entirety of the data collected about them through both internet services and hardware products like an Alexa-equipped Echo smart speaker. One German user, under the alias "Martin Schneider," did just that in August of this year. What he got back from Amazon, however, were thousands of Alexa voice recordings, which was strange considering he didn't own an Alexa device.

Upon listening to the files, Schneider discovered they were the recordings of another Alexa user. After failing to get in contact with Amazon about the issue, the man brought the files to *c't*, where reporters were able to piece together who the Alexa user was. Among the files were commands to control

Spotify, the person's home thermostat, and alarms. There were also recordings that indicated the Alexa user also owned a Fire TV, and that they had a spouse who appeared to live in the home.

Voice assistants like Alexa are always listening, and the data isn't always secure

"Using these files, it was fairly easy to identify the person involved and his female companion; weather queries, first names, and even someone's last name enabled us to quickly zero in on his circle of friends," the report reads. "Public data from Facebook and Twitter rounded out the picture." It turns out that the victim in this case also filed a data request under the new GDPR rules, *c't* reports, but somehow the two men received each other's reports.

"This was an unfortunate case of human error and an isolated incident. We have resolved the issue with the two customers involved and have taken steps to further improve our processes," an Amazon spokesperson told *The Verge*. "We were also in touch on a precautionary basis with the relevant regulatory authorities."

Like other tech companies, Amazon uses Alexa voice recordings both to personalize features and to improve the overall quality of its natural language processing skills and other artificial intelligence-assisted abilities. While it doesn't store much of the actual data on the device itself, it does store it in the cloud, and Amazon clearly makes that information available to EU citizens under GDPR. (It also makes that data available to law enforcement with the proper warrant, which is why Echo devices have found their way into domestic abuse and even murder trials in the past.)

Despite possessing a vast amount of personal data on its customers, Amazon has come under fire for similar privacy blunders in the past. An Echo device accidentally recorded an entire conversation between a Portland woman and her husband back in May, and then sent the conversation to a colleague of the husband's.

Apparently, Alexa initiated a series of commands, including to record the conversation as a voice message and then to send it to a random contact, on its own, while the couple was completely unaware. At the time, Amazon called the situation "unlikely" for the rarity that such a series of commands would trigger subsequently and without a user noticing, but it said it was "evaluating options to make this case even less likely." So it's not exactly reassuring to know that the microphones we now comfortably place in our bedrooms and bathrooms may be inadvertently sending that information to someone else, or in the case of Schneider, that a random stranger might receive it over email in a zip file.