Hot Clicks: Is Alexa Always Listening?

Rounding up IT and advanced tech-related news impacting government and industry.

Amanda Ziadeh

Tue, 05/29/2018 - 09:13

Illustration: ValeryBrozhinsky/iStock

We’ve always wondered if our digital home assistants were secretly listening on our private conversations without being called on or summoned. Privacy advocates warned us, and now it has happened, according to a women in Portland, Oregon.

She told a news station in Washington her Amazon Echo recorded a conversation and shared it with her husband’s employees. Creepy, right? Well, Amazon says Alexa mistakenly heard requests and commands as the woman and her husband spoke, and ended up sending the recording as a voice message. Apparently, Alexa “woke up” because the device thought it heard its name in the background conversation.

Then, there must have been a similar sound to “send message,” because Alexa responded out loud with “to whom?” and interpreted something in the conversation as a name in the customer’s contact list. Amazon then says Alexa confirmed the contacts name out loud, and then, again, interpreted background conversation as “right.” That’s quite a series of unfortunate events, Amazon, especially as the woman said Alexa never asked for her permission to send the audio. Needless to say, the couple unplugged their device. The New York Times

Twitter Verifies Political Candidates with Badge

In an effort to stop the spread of misinformation (ahem, 2016 U.S. presidential election), Twitter is adding a small government building icon next to political candidates before the start of the 2018 midterm elections. The badge will be accompanied by the position the candidate is running for and the state or district of the race. These “election labels” are meant to help users identify original sources and factual information, and will start appearing after May 30 for candidates in state governor races and those campaigning for a Senate or House seat.

To create the labels, Twitter is working with the nonpartisan political nonprofit Ballotpedia. The company said it covers all candidates in every upcoming election in the 100 most populated cities and all federal and statewide elections, so after each state primary, it’ll provide Twitter with governor and congressional candidates appearing on the November ballot.

And after getting the OK from each candidate, Twitter will attach those badges to each candidate profile. Verified political profiles, here we come! Tech Crunch

Europe a Step Ahead in Tech Privacy Regulations

Thanks to the May 25 implementation of a suite of new laws called the General Data Protection Regulation, Europe is regulating Silicon Valley more than the U.S., setting a global standard for how tech companies should handle customer data. In fact, it gives Americans new protections and our tech companies new limitations. But considering the country's concern of political influential companies, perhaps it's what we needed.

GDPR allows user to demand their data be deleted and to object to new kinds of data collection. The laws also require companies get full consent for how they collect, process and use data, and violators could face major fines. But GDPR doesn't directly limit how tech companies treat customers outside of Europe, so some companies are adopting the laws on their own and releasing new privacy policies.

This legal move has been driven by mistrust in Silicon Valley and recent private sector abuse of personal privacy — causing U.S. consumer advocates to threaten filing legal complaints in the E.U. against big American tech companies like Amazon and Facebook to change business practices. But Europe is more comfortable with government regulation of private companies than the U.S. is, so it may just be a matter of time before we get onboard. The Washington Post

Pentagon Releases More UFO Info

Remember that secret Defense Department program that investigated unidentified flying objects, the Advanced Aerospace Threat Identification program, that was exposed in December? We were gifted with the release of a video showing a white oval object being chased by two fighter jets off the California coast in 2004, and it became known as the "Tic Tac UFO." Well, an investigative news team in Las Vegas got its hands on a 13-page document analyzing what happened that day. It described how the Anomalous Aerial Vehicle in the video rapidly descended from about 60,000 feet to 50 feet in seconds, and it would hover for a bit and depart at "high velocities."

And before those two F18 fighter jets caught the AAV on film, the report said those same advanced characteristics were seen by another aircraft carrier off the coast of California three separate times. Those characteristics included "advanced acceleration, aerodynamic and propulsion capability," and, even weirder, "possibly demonstrated the ability to ‘cloak’ or become invisible to the human eye or human observation,” and “possibly demonstrated a highly advanced capability to operate undersea completely undetectable by our most advanced sensors,” according to the report.

Though it’s noted the AAV exhibited characteristics of a ballistic missile, but the aircraft radar system wasn’t on the right mode for ballistic missile tracking, so it wasn’t able to track the AAV. Regardless, it’s still an unsolved UFO mystery. Motherboard

Can AI Stop Fake News?

DOD’s Defense Advanced Research Projects Agency wants to find out, so it’s funding a project to discover if real-looking fake video and audio created by artificial intelligence will soon be indistinguishable from the real deal.

The project is essentially an AI fakery contest, and leading digital forensics experts will compete to develop the most convincing AI-generated fake video, imagery and audio this summer. And it goes both ways, as they’ll also try develop tools that can detect the counterfeits automatically.

Think videos where a person’s face is attached to another person’s body, like in fake celebrity porn videos. But this kind of artistry could also be used to create a clip of a politician saying or doing something crazy. DARPA’s also concerned about a new AI technique that uses generative adversarial networks, or GANs, that make AI counterfeits impossible to detect automatically because it’s so realistic. It’s a relatively new technique, but is taking machine learning by storm in the “deepfake” scene, and DARPA wants to learn its limits. MIT Technology Review

View printer friendly version
Amazon
Alexa
AI
UFO
Defense Department
privacy
news roundup
Artificial Intelligence

social media

GDPR

DARPA