

Business

Google failed to notify customers it put microphones in Nest security systems

By Taylor Telford

February 20

The worst kind of microphone is a hidden microphone.

Customers were caught off guard in early February when Google announced its home security system, Nest Secure, would be able to act as an AI-powered Google Assistant after a recent update.

“With the flip of a switch in the Nest app, you can set the Secure as an always-listening Assistant speaker,” the company said [in a blog post](#) announcing the update.

Until then, customers weren’t aware that Nest Secure had a microphone at all.

Google said it had made an “error” in failing to include the microphone in technical specifications, [Business Insider first reported](#). Nest Secure had been on the shelves for 18 months. The company did mention the microphone in an announcement on February 4, according to a press release, saying it was “not enabled by default.”

CONTENT FROM AT&T BUSINESS 

Flexible tech solutions can prepare your business for nearly any challenge, but first you need a game plan.



[Read More](#)

CONTENT FROM AT&T BUSINESS 

Flexible tech solutions can prepare your business for nearly any challenge, but first you need a game plan.

“The on-device microphone was never intended to be a secret and should have been listed in the tech specs,” Google said in a statement emailed to The Post. “That was an error on our part. The microphone has never been on and is only activated when users specifically enable the option.”

The microphone was included to leave the door open for additional features to be added to the technology, Google said, like the ability to detect broken glass. The company said sound sensing devices are common in security systems. Google introduced a similar voice-driven functionality to Nest’s security camera last year.

In the blog post, Google said that many people may not need the Google Assistant functionality because most already have separate devices for those purposes. The company explained that the range of the voice-command functions would be also limited — the system can’t play music or be disarmed with a voice.

ADVERTISING



But many people were unsettled by the possibility of Google having access to homes without customers’ knowledge.

“Nest’s failure to disclose the onboard microphone included in its secure home security system is a

massive oversight,” said Ray Walsh, a digital privacy expert at BestVPN.com. “Despite Google’s assurances, the fact is that the device has a microphone which could potentially have been hacked or accessed by Google to perform covert corporate surveillance.”

Tensions around privacy practices have risen since it was discovered that Facebook had allowed developers to access users data, and that 87 million users had their data compromised by political consultancy firm Cambridge Analytica. In Senate hearings in September, tech leaders from Google and Apple told lawmakers it was time for [federal privacy legislation](#) after many had pushed against such measures.

Google has also come under fire for its privacy practices in the past. An investigation [by the Associated Press](#) in August revealed Google had been recording customers’ location information in Android phones, even if they had opted out of tracking.

Google bought the smart home appliance company, Nest Labs, in a \$3.2 billion deal in 2014. The company had been operating as a separate business under parent company Alphabet. In February 2018, it became part of Google’s hardware division, which makes Google Home technology and Pixel smartphones.

Taylor Telford

Taylor Telford is a reporter covering national and breaking news. Follow [Twitter](#)



The Washington Post

Be the first to know.

Try 1 month for ~~\$10~~ \$1

Send me this offer

Already a subscriber? [Sign in](#)