

Search Labs



SUBSCRIBE

[NEWS](#) | [PRIVACY](#)

This site uses cookies in order to enhance site navigation, analyze site usage and marketing efforts. Please see our privacy policy for more information.

[Privacy Policy](#)[Cookies Settings](#)

Decline All

Accept All Cookies





While collecting data on users is nearly inevitable in today's corporate world, secret, undisclosed, or unpredictable data collection—or data collection abilities—is another problem.

A smart-home speaker shouldn't be secretly hiding a video camera. A secure messaging platform shouldn't have a government-operated backdoor. And a home security hub that controls an alarm, keypad, and motion detector shouldn't include a clandestine microphone feature—especially one that was never announced to customers.

And yet, that is precisely what Google's home security product includes.

Google fumbles once again

Last month, Google announced that its Nest Secure would be updated to work with Google Assistant software. Following the update, users could simply utter "Hey Google" to access voice controls on the product line-up's "Nest Guard" device.

The main problem, though, is that Google never told users that its product had an internal microphone to begin with. Nowhere inside the Nest Guard's hardware specs, or in its marketing materials, could users find evidence of an installed microphone.

When Business Insider broke the news, Google fumbled ownership of the problem: "The on-device microphone was never intended to be a secret and should have been listed in the tech specs," a Google spokesperson said. "That was an error on our part."

Customers, academics, and privacy advocates balked at this explanation.

"This is deliberately misleading and lying to your customers about your product," wrote Eva Galperin, director of cybersecurity at Electronic Frontier Foundation.

"Oops! We neglected to mention we're recording everything you do while fronting as a security device," wrote Scott Galloway, professor of marketing at the New York University Stern School of Business.

The Electronic Privacy Information Center (EPIC) spoke in harsher terms: Google's disclosure

This site uses cookies in order to enhance site navigation, analyze site usage and marketing efforts. Please see our privacy policy for more information.

[Privacy Policy](#)



AS consumer technology becomes ever more advanced, it is essential that consumers know the capabilities of the devices they are bringing into their homes so they can make informed choices,” [the letter said](#).

This isn't just about user data

Collecting user data is essential to today's technology companies. It powers Yelp recommendations based on a user's location, product recommendations based on an Amazon user's prior purchases, and search results based on a Google user's history. Collecting user data also helps companies find bugs, patch software, and retool their products to their users' needs.

But some of that data collection is visible to the user. And when it isn't, it can at least be learned by savvy consumers who research privacy policies, read tech specs, and compare similar products. Other home security devices, for example, advertise the ability to trigger alarms at the sound of broken windows—a functionality that demands a working microphone.

Google's failure to disclose its microphone prevented even the most privacy-conscious consumers from knowing what they were getting in the box. It is nearly the exact opposite approach that rival home speaker maker Sonos took when it installed a microphone in its own device.

Sonos does it better

In 2017, Sonos revealed that its newest line of products would eventually integrate with voice-controlled smart assistants. The company opted for transparency.

Sonos updated its privacy policy and [published a blog about the update](#), telling users: “The most important thing for you to know is that Sonos does not keep recordings of your voice data.” Further, Sonos eventually designed its speaker so that, if an internal microphone is turned on, so is a small LED light on the device's control panel. These two functions cannot be separated—the LED light and the internal microphone are hardwired together. If one receives power, so does the other.

This site uses cookies in order to enhance site navigation, analyze site usage and marketing efforts. Please see our privacy policy for more information.

[Privacy Policy](#)



a company failing to respect the privacy of its users.

A microphone in a home security product may well be a useful feature that many consumers will not only endure but embrace. In fact, internal microphones are available in many competitor products today, proving their popularity. But a secret microphone installed without user knowledge instantly erodes trust.

As we showed in our recent [data privacy report](#), users care a great deal about protecting their personal information online and take many steps to secure it. To win over their trust, businesses need to responsibly disclose features included in their services and products—especially those that impact the security and privacy of their customers' lives. Transparency is key to establishing and maintaining trust online.

SHARE THIS ARTICLE



Malwarebytes Labs Comment Policy

All comments are moderated. Relevant comments will be published and all URLs will be removed.

Got it

What do you think?

0 Responses



0

Upvote



0

Funny



0

Love



0

Angry



0

Sad

This site uses cookies in order to enhance site navigation, analyze site usage and marketing efforts. Please see our privacy policy for more information.

[Privacy Policy](#)

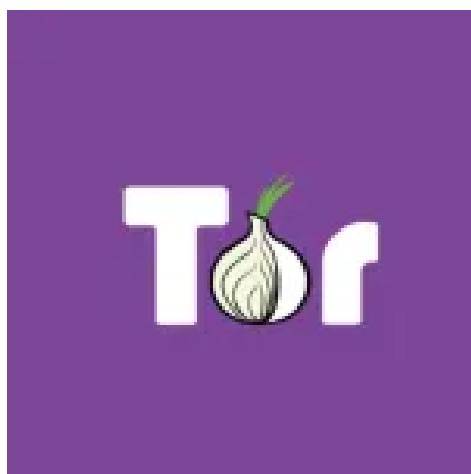


23andMe will retain your genetic information, even if you delete the account

October 17, 2024 - Sure, you can request a deletion of your data from 23andMe, but that doesn't mean the company will delete it entirely.

[CONTINUE READING](#)

0 Comments



Tor Browser and Firefox users should update to fix actively exploited vulnerability

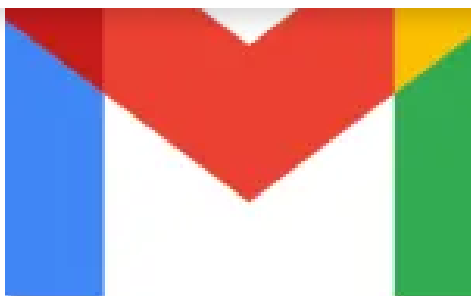
October 16, 2024 - Mozilla warns that a vulnerability in Firefox and Tor Browser is actively being exploited against both browsers

[CONTINUE READING](#)

0 Comments

This site uses cookies in order to enhance site navigation, analyze site usage and marketing efforts. Please see our privacy policy for more information.

[Privacy Policy](#)

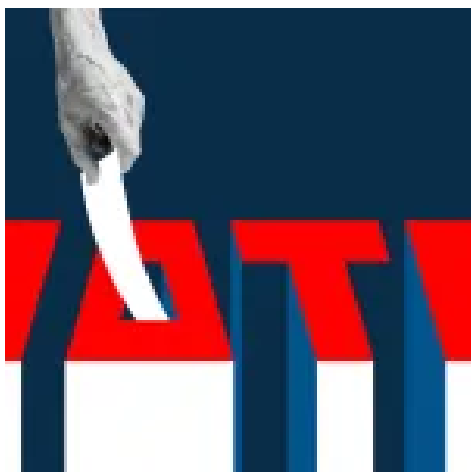


accounts, say they have your death certificate

October 15, 2024 - Typical AI supported scams are after your Google account by pretending to follow up on account recovery requests

[CONTINUE READING](#)

1 Comment



Personal | Privacy

Election season raises fears for nearly a third of people who worry their vote could be leaked

October 15, 2024 - The US presidential election is stirring fears amongst a third of people who worry that their vote could be exposed to outsiders.

[CONTINUE READING](#)

0 Comments



Exploits and vulnerabilities | News

This site uses cookies in order to enhance site navigation, analyze site usage and marketing efforts. Please see our privacy policy for more information.

[Privacy Policy](#)

ABOUT THE AUTHOR



David Ruiz 

Pro-privacy, pro-security editor. Former journalist turned advocate turned cybersecurity defender. Still a little bit of each. Failing book club member.



Contributors



Threat Center



Podcast



Glossary



Scams



Cyberprotection for every one.

Cybersecurity info you can't live without

This site uses cookies in order to enhance site navigation, analyze site usage and marketing efforts. Please see our privacy policy for more information.

[Privacy Policy](#)

[Windows Antivirus](#)[Mac Antivirus](#)[Android Antivirus](#)[Free Antivirus](#)[VPN App \(All Devices\)](#)[Malwarebytes for iOS](#)[SEE ALL](#)[Small Businesses](#)[Mid-size Businesses](#)[Larger Enterprise](#)[Endpoint Protection](#)[Endpoint Detection & Response \(EDR\)](#)[Managed Detection & Response \(MDR\)](#)

COMPANY

[About Us](#)[Contact Us](#)[Careers](#)[News and Press](#)[Blog](#)[Scholarship](#)[Forums](#)[Vulnerability Disclosure](#)

FOR PARTNERS

[Managed Service Provider \(MSP\) Program](#)[Resellers](#)

MY ACCOUNT

[Sign In](#)

SOLUTIONS

LEARN

This site uses cookies in order to enhance site navigation, analyze site usage and marketing efforts. Please see our [privacy policy](#) for more information.

[Privacy Policy](#)



ADDRESS

One Albert Quay
2nd Floor
Cork T12 X8N6
Ireland



[Legal](#)

[Privacy](#)

[Terms of Service](#)

[Accessibility](#)

[Imprint](#)

© 2024 All Rights Reserved

This site uses cookies in order to enhance site navigation, analyze site usage and marketing efforts. Please see our privacy policy for more information.

[Privacy Policy](#)