New American

Written by **C. Mitchell Shaw** on August 5, 2020

Google Home "Smart" Speaker Caught Spying on Users

The popular Google Home "smart" device that allows users to perform voice searches and automate other "smart" devices in their homes has just been caught spying on users. While this comes as no surprise to privacy advocates who have long warned others this was the case, it is now an incontrovertible fact.

As the *Independent* reported Tuesday, a user on Reddit posted that his Google Home "smart" speaker sent a notifaction to his phone that his smoke alarm was going off in his house. The problem? It was not a "smart" Internet-connected smoke alarm, but a cheap $10 "dumb" alarm. The notification was sent because the Google Home speaker heard the alarm going off and recognized it.

That, of course, means that — as this writer has said before — the device is always listening. And contrary to popular belief and Google's previous claims, it is not just listening for the typical "O.K. Google" and "Hey, Google" commands. It is simply *always listening* and sending what it hears to Goggle's servers.

And while that user saw the intrusion as a benefit — posting "Pretty rad google" — the implications are staggering. This is what this writer calls surveillance-as-a-feature.

As the *Independent* reported, that user was not alone in this strange experience:

> Other users reported getting alerts for the sound of glass breaking, popped bubble wrap, an air compressor tank, and other high-pitched noises that sound like alarms.

Once the creepy surveillance aspect of the device was found, Google attempted to explain it way. As the *Independent* reported:

> In a statement to Protocol, a Google spokesperson said that the feature was accidentally enabled through a recent software update which has now been reversed.

Wait, did you catch that? Google's explanation (read: excuse) is that this was caused by an update that "accidentally" turned on a feature. Here is a pro tip for the folks over at Google: If the "feature" did not exist in the first place, it could not have been "accidentally" activated. And there is the rub.

This all dates back to a previous report of Google's vision for the future of "smart" home devices. As this writer reported in November 2018, Google had filed patents to accomplish exactly what it now claims was an accident:

> According to recently disclosed patents, Google is preparing to take "surveillance as a feature" to a whole new level, with devices in every room of users' homes to watch, listen, and analyze users' every word and action.

That previous article reveals that the text of those patents shows Google's too-much-is-never-enough attitude toward your personal data:

> The recently publicized patents reveal that the surveillance hawks at Google apparently don't think enough is enough. In fact, those patents show that the new technology in Google's offing blows past anything the company has done up to this point. The new technology includes the integration of cameras, microphones, and other sensors that would allow those devices to work together to monitor the comings and goings (using sensors on doors as well as cameras and microphones) of people in homes equipped (read: bugged) with the devices. The cameras and microphones would allow the devices and Google's servers to recognize people and objects and analyze the significance of the presence of those people and objects.

And, quoting from the patents themselves:

> Paragraph [0003] and [0004] state:
>
> > People interact with a number of different electronic devices on a daily basis. In a home setting, for example, a person may interact with smart thermostats, lighting systems, alarm systems, entertainment systems, and a variety of other electronic devices. Unfortunately, the usefulness of these devices often times is limited to basic and/or particular pre-determined tasks associated with the device.
> >
> > As society advances, households within the society may become increasingly diverse, having varied household norms, procedures, and rules. Unfortunately, because so-called smart devices have traditionally been designed with pre-determined tasks and/or functionalities, comparatively fewer advances have been made regarding using these devices in diverse or evolving households or in the context of diverse or evolving household norms, procedures, and rules.
>
> And paragraph [0006] says:
>
> > According to embodiments of this disclosure, a smart-home environment may be provided with smart-device environment policies that use smart-devices to monitor activities within a smart-device environment, report on these activities, and/or provide smart-device control based upon these activities.

So, while Google — a surveillance company masquerading as a search engine/tech company — claims this recent episode was an accident, it is plain that this "accident" has been long in the planning. The company's dog-eared excuse of "software bugs" and "accidental" glitches caused by upgrades is getting tired and thin. Another case in point: Three months after this writer reported on the Google patents described above, Google put hidden microphones in Nest "smart" home alarm systems and did not inform users of the microphones. Nothing on the packaging, the manual, or any advertising made any mention of the microphones.

Their excuse? It was an "error."

As the *Independent* states in its report on this new "accidental" spy feature:

> Although the feature provides greater security it is a trade off for less privacy. Google has adamantly pushed that the only way its smart speaker will listen to users is via its wake word.
>
> The use of ambient monitoring for other reasons could lead to questions about what else Google will request to monitor in the future — especially since all that stands in the way of a users'

> acquiescence is a privacy policy that few will ever read.

The *Independent* goes on to address that Google is not the only company creating creepy "smart" devices, referring to a 2018 report of Amazon's Echo and its Alexa Guard "feature." And as this writer reported at the beginning of the COVID-19 lockdown that led to many employees working from home, lawyers told employees to turn off such devices in their homes. Why? Because of confidentiality concerns.

And another previous report by this writer illustrates that — as early as May 2018 — this was a known issue. As that article explained, a Portland family was having a private conversation in their Echo-equipped home when their Echo recorded the conversation, zipped up the file, randomly selected a contact from their list of contacts, and emailed the sound file to him.

The take-away from all of this should be obvious. Ditch so-called smart devices that are Internet-connected and can (and will) be used to spy on your privacy. And if you wonder why this matters if you "have nothing to hide," this writer has answered that question here and here.

And since you are reading this and others may not be, share this article with them. Friends don't let friends get spied on.

Image: wallpaperflare.com

C. Mitchell Shaw is a freelance writer and public speaker who addresses a range of topics related to liberty and the U.S. Constitution. A strong privacy advocate, he was a privacy nerd before it was cool. He hosts and produces the popular Enemy of the [Surveillance] State podcast.