It’s Not Just Ring. Google, SimpliSafe, and Others Could Share Video Footage With Police Without Consent.

Federal law allows it, but there are security cameras with stronger privacy protections

By Daniel Wroclawski

Published July 28, 2022 | Updated May 2, 2023

Photo: Google, TP-Link, SimpliSafe

The role of video doorbells and security cameras in aiding police investigations has become a hot topic over the past few years, with privacy advocates arguing against relationships between law enforcement and companies that store residential security-camera video.

While much of the focus has been on Amazon’s Ring, a subsequent review of privacy policies and terms of service at Eufy, D-Link, Google, SimpliSafe, and TP-Link reveals that all have policies for sharing camera and doorbell video footage with law enforcement without a warrant or user permission, in the event of potentially life-threatening emergencies, or to protect the safety of individuals.

Even companies without these policies (such as Arlo, ADT, and Wyze) can share video with law enforcement under an exception in the federal Electronic Communications Privacy Act (ECPA).

This federal law states that providers can disclose customer records “to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency.”

Google—which has a Law Enforcement Request System for these requests—confirmed its policy with Consumer Reports, citing the legal powers granted to it under the ECPA. Eufy and SimpliSafe confirmed they have similar policies. D-Link and TP-Link did not respond to requests for comment, although their policies are spelled out on their respective websites.

CR reached out to these companies last year after Amazon disclosed that it shares Ring camera and doorbell footage with the police without warrants in emergency situations, and did so 11 times in the first half of 2022.

Among the other companies with emergency request policies, Eufy told CR in July 2022 that it had received two law enforcement requests in the previous year, but it couldn't comply because the footage was stored locally on the Eufy cameras, not in Eufy's cloud storage system. Google and SimpliSafe claimed in July 2022 that they hadn't used their policies to date.

"We take emergency disclosure requests very seriously, and have dedicated teams and strict policies in place that are designed to ensure that we provide information that can assist first responders in the event of an emergency while ensuring that we only disclose data that is reasonably necessary to avert an ongoing threat," a Google spokesperson says.

How You Store Your Camera Footage Matters

It's worth noting that these policies specifically apply to Google, Eufy, D-Link, TP-Link, and SimpliSafe cameras and doorbells that store footage on the manufacturers' servers.

While all Google Nest and SimpliSafe cameras and doorbells use cloud video storage, most Eufy cameras and doorbells store footage locally on the device itself using end-to-end encryption, with the company's cloud video storage being an optional service for Eufy customers. (A reported vulnerability that exposed livestreams of some customers' cameras was fixed by the company in early 2023.) Some D-Link and TP-Link cameras can store footage locally on a microSD card, but other models from each brand require cloud video storage plans.

"With Eufy Security, our user's video footage is stored locally and privately in their homes. We do not have access to this footage," says a Eufy spokesperson, Vicky Guo. "We do offer optional cloud storage for those that want to expand their storage capacity, but this applies to less than 2 percent of our customer base."

Guo added that "in those rare cases where we might be storing a user's footage in our optional cloud service," Eufy will share the footage with law enforcement with user consent, under a legally binding order, or in "an emergency involving imminent danger of death or serious physical injury to a person." A SimpliSafe spokesperson, Amy Nagy, says: "In our privacy policy we do reserve the right to share customer videos with law enforcement in times of extreme emergencies. Having this in our privacy policy

does not change our practice of not sharing this data with law enforcement unless required to do so by law," or with user consent in most cases.

Google's policies similarly allow it to share video with law enforcement where there is user consent or a legal order, while D-Link's and TP-Link's policies will do so under legal orders. (Their documentation doesn't mention user consent.)

"Nobody is telling Amazon, Google, Eufy, and others that they're required to share user video with law enforcement," says Anna Bonesteel, strategic response manager for the privacy advocacy group Fight for the Future. "The federal law cited by Google states that companies 'may' disclose customer records without permission. It doesn't say they 'must.'"

"But these companies are giving up private video to the police anyway—without a warrant, without permission, and without notification," they added. "Amazon Ring created the market for these every-household surveillance devices, so they arguably deserve the most blame for establishing industry-standard policies that circumvent our individual rights."

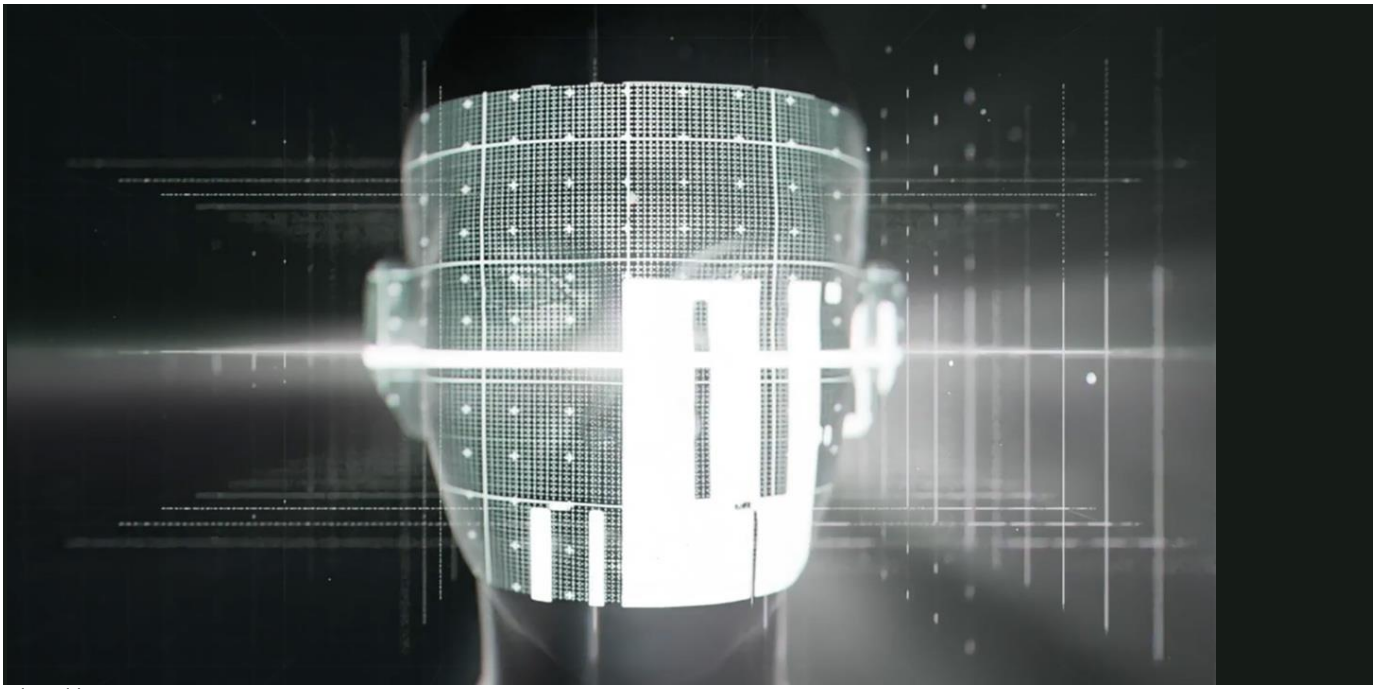
Greg Nojeim, senior counsel at the Center for Democracy and Technology, says the emergency exception outlined by ECPA isn't necessarily a bad thing, because there are noncriminal emergencies that could benefit from these disclosures.

Asked to describe a real-life scenario where these disclosures can be helpful, Nojeim says to imagine that it's 2 a.m. and an elderly grandmother has wandered off. Her daughter calls the police, who want to check the home's security cameras to know when she might have left and which direction she headed. There's no suspicion of crime, so it is not possible to get a warrant, and the camera account owner, the daughter's husband, is out of town and can't be reached. In this case, the police would contact the camera maker, describe the emergency, and get disclosure of the footage under the emergency exception.

"The trick is for providers to get it right and make sure the emergency exception in ECPA isn't being abused by law enforcement and used to circumvent the warrant requirements," Nojeim says.

BAD INPUT: Facial Recognition

Watch a short film about privacy issues raised by this technology.



Play Video

How to Avoid Emergency Disclosures

If you don't want home security companies giving your footage to the police under the Electronic Communications Privacy Act, you have a few options.

Arlo told CR that it doesn't share video with law enforcement in emergency situations unless there's user consent or a legally binding order. An ADT spokesperson told CR that "ADT's policy is not to share customer video with law enforcement without our customer's consent, except pursuant to a lawful order or as otherwise required by law."

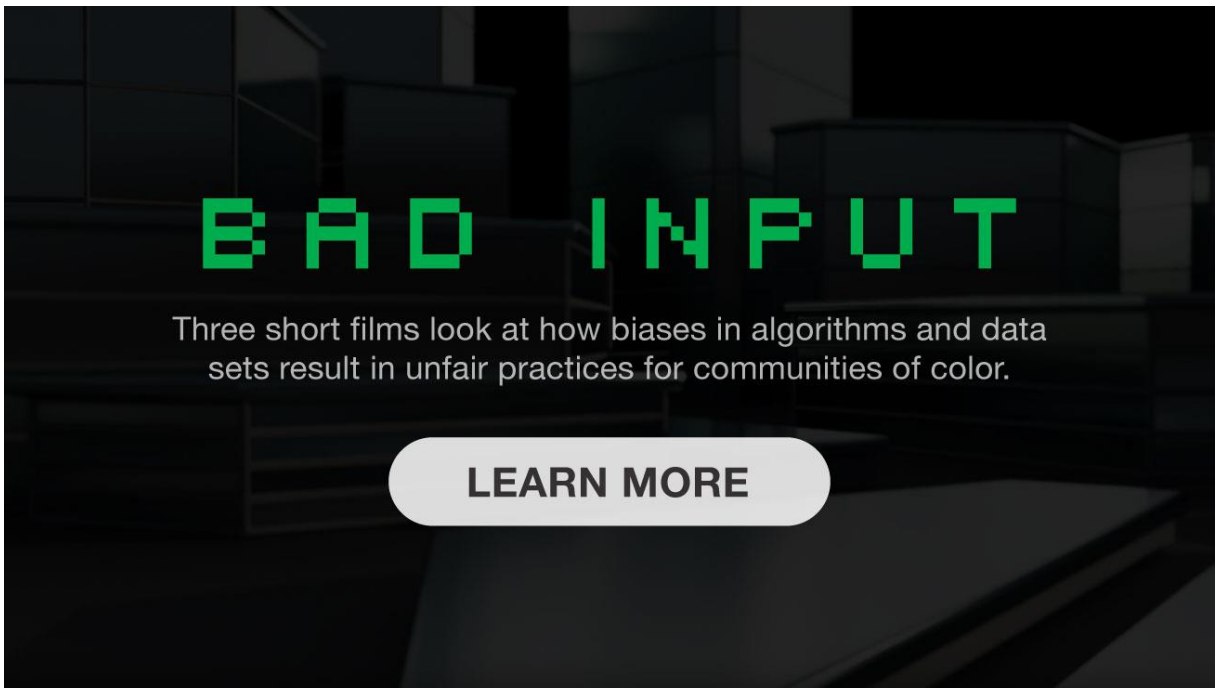
A Wyze spokesperson says, "We only share if law enforcement provides a valid subpoena or warrant." While ADT and Wyze didn't explicitly state they don't provide footage in emergency situations, we couldn't find any policy to the contrary in their legal documentation.

Another option is to use security cameras and video doorbells with local video storage. That way, law enforcement has to come to you directly to ask for footage or serve a warrant. As mentioned above, most Eufy cameras and doorbells use local storage, as do Wyze cameras (though not its doorbells), Netatmo cameras and doorbells, some D-Link cameras, and some TP-Link cameras and doorbells.

Finally, if you want cloud storage but still want to have complete control over your video, you could opt for a camera or doorbell that uses Apple HomeKit Secure Video to store video in Apple iCloud.

A key feature of HomeKit Secure Video is end-to-end encryption, meaning that your video footage can be accessed only from your personal Apple devices. Neither Apple nor the camera manufacturer can access your footage, even if it wants to do so. If law enforcement wants access to your video in this instance, they will have to come to you directly.

Cameras and doorbells that support Apple HomeKit Secure Video include the Eufy Cam 2C Pro, Eufy Solo IndoorCam C24, Eve Indoor Cam, Logitech Circle View Camera, Logitech Circle View Doorbell, and Wemo Smart Video Doorbell.



Daniel Wroclawski

Dan Wroclawski is a home and appliances writer at Consumer Reports, covering products ranging from refrigerators and coffee makers to cutting-edge smart home devices. Before joining CR in 2017, he was an editor at USA Today's Reviewed, and launched the site's smart home section. In his spare time, you can find him tinkering with one of the over 70 connected devices in his house. Follow Dan on Facebook and Twitter @danwroc.