New American

Written by **Joe Wolverton, II, J.D.** on January 31, 2020

Amazon Software Engineer Calls for Recall of Ring Devices, Citing Security Breaches

https://media.blubrry.com/1462062/mcdn.podbean.com/mf/web/h38aai/Amazon_Software_Engineer_Calls_for_Recall_of_Ring_Devices_Citing_Security_Breaches.mp3
Podcast: Play in new window | Download ()
Subscribe: Android | RSS | More

An Amazon software engineer is calling for the shutdown of Ring, Amazon's smart doorbell and surveillance device, explaining that the service is incompatible with privacy.

Max Eliaser, the Amazon employee insisting that the connected Ring doorbells and cameras should be shelved, posted an explanation on Medium. "The deployment of connected home security cameras that allow footage to be queried centrally are simply not compatible with a free society. The privacy issues are not fixable with regulation and there is no balance that can be struck. Ring should be shut down immediately and not brought back," he wrote.

Eliaser isn't alone in raising a warning voice about the potential threats to privacy posed by the popular doorbell camera. The Electronic Frontier Foundation (EFF) published a report revealing substantial breaches to the privacy of users of the Amazon-owned "smart" technology. EFF's report showed the smart device is a lot savvier than users likely realize:

> Ring doorbell app for Android found it to be packed with third-party trackers sending out a plethora of customers' personally identifiable information (PII). Four main analytics and marketing companies were discovered to be receiving information such as the names, private IP addresses, mobile network carriers, persistent identifiers, and sensor data on the devices of paying customers.

While Amazon does not publish sales numbers, industry insiders estimate that the online retailer has sold over 400,000 units of the Ring devices, which include doorbell cameras and in-home surveillance cameras and microphones.

Regarding the Ring doorbell app, the EFF investigation disclosed a shocking amount of personal data is shared with third-party companies without notice to the user.

> AppsFlyer, a big data company focused on the mobile platform, is given a wide array of information upon app launch as well as certain user actions, such as interacting with the "Neighbors" section of the app. This information includes your mobile carrier, when Ring was installed and first launched, a number of unique identifiers, the app you installed from, and whether AppsFlyer tracking came preinstalled on the device. This last bit of information is presumably to determine whether AppsFlyer tracking was included as bloatware on a low-end Android device.
>
> Most alarmingly, AppsFlyer also receives the sensors installed on your device (on our test device, this included the magnetometer, gyroscope, and accelerometer) and current calibration settings.

As unbelievable as that relationship is, AppsFlyer is not the biggest benefactor of Ring's data sharing scheme.

More from EFF's report:

> Ring gives MixPanel the most information by far. Users' full names, email addresses, device information such as OS version and model, whether bluetooth is enabled, and app settings such as the number of locations a user has Ring devices installed in, are all collected and reported to MixPanel. MixPanel is briefly mentioned in Ring's list of third party services, but the extent of their data collection is not.

What makes this data-sharing arrangement even more menacing is that the method of encryption used by Amazon makes it difficult for someone trying to detect the presence of the programs that gather and send the data. Security companies or researchers that might be looking for such security breaches would find these barricades, impediments that would likely discourage digging any deeper.

Beyond the app-based breach of privacy, the Ring devices create situations where surveillance can be conducted of people who don't have the service and who cannot keep themselves from being watched by those who do.

Amazon's Ring home security service has entered into contracts with over 200 police departments, giving law enforcement expansive access to the video and audio collected by the service's surveillance devices.

A visit to Amazon's Ring Security System's product page reveals to possible customers — and those worried about personal privacy — all the data that Amazon is making available, without prior permission or notice of Ring customers, to police departments.

Monitor your property in HD video, and check-in on home at any time with Live View on-demand video and audio.

Hear and speak to people on your property from your mobile device with the built-in microphone and speakers.

Activate the siren from your phone, tablet, and PC to scare away any suspicious people caught on camera.

This threat could damage more than just neighborhood barbecues.

Let me offer the following frightening use of user-provided surveillance video footage: Two neighbors are arguing for months over some matter and the disagreement has escalated to a heated exchange of words. Now imagine that one of the neighbors subscribes to Amazon's Ring security system and he knows that he can give cops access to the images recorded by his Ring surveillance camera. He reviews the footage and finds an image of his neighbor trying to get into a car the neighbor owns, but accidentally locked himself out of. The car is parked on the street between the two houses.

Now, imagine you're the neighbor trying to get into your own car and you see a picture of yourself on Twitter posted by Amazon carrying the caption: "This man was caught on video breaking into a vehicle."

Imagine that the neighbor's employer sees the ad and decides that he doesn't want to employ "a criminal."

Perhaps most troubling is the fact that the images and sounds recorded by Ring can be obtained from Ring customers without a warrant. Admittedly, the homeowner would need to give permission to police, but pressure would be there. As millions of Americans are fond of saying, "If you haven't done anything

wrong, you've got nothing to hide." So complying with a request from police for access to their security camera footage would be regarded by many as their civic duty.

Although the Ring cameras were originally marketed as a way to see who's standing outside the door before opening it, many users have installed the surveillance equipment inside the house.

Amazon has admitted that on at least four occasions, Amazon employees have accessed the live feeds of video and audio collected by Ring devices installed inside of customers' homes.

Finally, Amazon's Ring devices are so vulnerable that hackers have managed to get control of them and communicate with customers from inside their own homes!

With all of these examples of how the Amazon Ring smart devices are susceptible to such insidious invasions of privacy, much of which is being done either knowingly by the company without disclosing the data sharing to customers, it is little wonder that one of Amazon's own software engineers is publicly calling for the tech behemoth to pull the plug on this popular device.

Photo: scyther5 / iStock / Getty Images Plus