Uploaded Ring footage reportedly provides location to the square inch

Enlarge / A Ring camera doorbell.

reader comments

141 with 75 posters participating, including story author

Share this story

Amazon’s aggressive push to grow its surveillance-camera company Ring is working, and adoption has skyrocketed in the past two years thanks to deals with hundreds of police departments. A new set of reports highlights the ways Amazon convinces police to join those partnerships—and the amount of data that users can inadvertently reveal.

Integral to the Ring system is an app called Neighbors, kind of like an over-eager NextDoor with everything except the crime stripped out. Neighbors generates a map of your local area, based on your address, and then populates it with crime reports. Those reports include comments from other Neighbors users, as well as reports of burglaries, vehicle break-ins or theft, shots fired or shootings, stabbings, hostages taken, and arson imported from real-time 911 dispatcher data.

Anyone can install the app and create an account, but owners of Ring devices can also upload video snippets to the service, either when they have something they want to share or when police request it using the companion portal for law enforcement. Gizmodo this week published a new report delving

into video data available on Neighbors to identify precisely how many Ring cameras are deployed, and where.

Too many to count

Gizmodo conducted its analysis in November, using videos posted to Neighbors in the previous 500 days—since right around July 1, 2018, give or take. The report managed to grab the precise locations of about 20,000 Ring cameras in nine-square-mile zones of 15 different US cities. Gizmodo adds that the reporters don't actually know how many camera locations they *could* have obtained, because they stopped collecting the data once they had enough information to generate their report.

In a location selected at random in Washington, DC, for example, Gizmodo was able to identify at least 1,863 unique Ring cameras that had uploaded video to Neighbors during the 500-day window. In their 9-square-mile sample of Los Angeles, they found at least 5,016 Ring cameras; in Denver, 1,788.

Gizmodo writes:

> *Examining the network traffic of the Neighbors app produced unexpected data, including hidden geographic coordinates that are connected to each post—latitude and longitude with up to six decimal points of precision, accurate enough to pinpoint roughly a square inch of ground.*

Many of those coordinates were indeed right in front of someone's house, a few feet away from the location of the camera. Some were near intersections; the farthest Gizmodo identified was about 260 feet. However, they note, backtracking to find the camera that captured footage is "trivial" in person, when armed with the video and the coordinates, and reporters basically drove or walked up to people's houses to prove it.

Ring did not refute Gizmodo's location findings, the site reports. Instead, the company said, "Only content that a Neighbors user chooses to share on the Neighbors App is publicly accessible through the Neighbors App or by your local law enforcement."

Gizmodo also spoke with a researcher at the Massachusetts Institute of Technology who has used several years' worth of video posted to Neighbors to make a similar map. He has so far pinpointed the locations of about 440,000 Ring cameras.

Ring did not refute that it was possible for anyone, armed with the data Gizmodo acquired, to pinpoint the exact locations of users' homes. Instead, the company reiterated that "Only content that a Neighbors user chooses to share on the Neighbors App is publicly accessible through the Neighbors App or by your local law enforcement."

What privacy?

When neighborhoods are blanketed with surveillance cameras, the privacy implications are profound. And because these cameras belong to individuals, there are few if any restrictions on what footage can be captured or used.

In Washington, DC, for example, Gizmodo notes that at least 13 active Ring cameras line the path between one public charter school for grades 6-12 and the soccer field its students use. Gizmodo also found several dozen instances of DC residents using Neighbors to share videos of children. Some of the kids in question were reportedly doing such activities as riding bicycles and taking selfies. Not exactly striking threats to public safety—but in a densely urban environment such as the District of Columbia, perhaps the homeowners simply did not have lawns to tell the kids to get off of.

Security and surveillance experts voiced concerns to Gizmodo that such a web of cameras could easily track individuals

going into or out of “sensitive buildings.” So the reporters looked and did indeed find at least one health clinic that provides abortion services within “unnerving proximity” to some Ring cameras, as well as a legal office handling immigration and refugee cases. Having footage showing individuals going to those sorts of facilities uploaded to a platform like Neighbors and becoming widespread could actually put individuals’ lives in danger.

https://arstechnica.com/?p=1630675