



Amazon Bonds With Law Enforcement Over Ring Cameras

Amazon is providing police with blanket surveillance in neighborhoods but homeowners bear the cost of installing its Ring cameras that replace doorbells with Internet connected cameras. Privacy? Forget it! □ TN Editor

On July 12, a few hours before dawn, a man in Chandler, Arizona, was jolted awake by an alert on his phone. It was coming from his Ring security camera, which had detected movement outside his home.

The live feed showed a group of young men breaking into cars. The man hollered at them through his front door, then called the police.

As an officer arrived, the men sped off in a car, leaving behind cellphones, tools and other things they'd taken during their interrupted burglary spree. They abandoned the getaway vehicle in a housing complex and turned themselves in later that morning.

By then, the homeowner had showed police his camera footage and

posted it to Neighbors, an app run by Ring, which is owned by Amazon. Ring doesn't just make the wireless security cameras — it also accesses police data to alert residents of potential crimes, encourages users to share recordings of suspicious behavior themselves, and connects them with law enforcement.

“Thank goodness for the Ring!!!” the man wrote on Neighbors.

“Thanks for posting,” a Chandler police officer responded.

The exchange was typical of the way police are using Ring, helping it spread its business while using it to detect and investigate crime. The arrangement in Chandler is among dozens of such partnerships around the country, and part of a much broader effort by Amazon to deepen its reach into law enforcement — which critics say is expanding the government's surveillance of Americans.

Amazon, known mainly for its online consumer marketplace, is becoming a potent resource for federal, state and local authorities, peddling an array of tools that harness the power of cloud-based computing, artificial intelligence and video analysis.

Some of the products seem mundane, offering agencies a relatively cheap method of storing, sharing and crunching data through networks of remote web servers known as the cloud. Others are contentious, making it easier for police to identify and monitor people. Together, they show how one company has broadened its influence by supplying law enforcement with technology that has modernized crime-fighting but is evolving too fast for government oversight to keep up.

Amazon's government work has become a significant component of the company's move beyond e-commerce and into tools that run the internet. Its government contracts, through the company's cloud-computing subsidiary, Amazon Web Services, have ballooned from \$200 million in 2014 to \$2 billion today, said Daniel Ives, who researches Amazon at the financial advisory firm Wedbush Securities. That has allowed the company to build “a fortress of cloud deals” that include police departments, federal law enforcement, national intelligence agencies and immigration authorities.

“In so many investigations, time is of the essence, and this enables many police departments to access data so much more quickly and in forms that are much more helpful,” Ives said.

But critics say Amazon’s products and services also show how a corporation can position itself within government in ways that could lead to overreach and abuse.

Privacy and civil liberties advocates have warned that the Ring partnerships [are creating a new layer of government surveillance](#). Amazon [employees](#), [artificial intelligence researchers](#) and [activist investors](#) have asked the company to stop selling its facial recognition service to law enforcement, to stop providing web-hosting services that help federal immigration authorities, and to create a committee that would [review the potential societal consequences](#) of its products.

“While providing secure cloud storage does not appear to pose privacy threats, providing a package of technologies that includes powerful surveillance tools like facial recognition and doorbell cameras, plus the capability to pool data into a massive database and run data analytics, does create very real privacy threats,” said Sharon Bradford Franklin, policy director of New America’s Open Technology Institute, a nonprofit that advocates for digital rights.

For example, Franklin said, a homeowner might voluntarily share the footage from their doorbell camera with police seeking clues to a nearby crime. The police might then run the video through facial recognition software, which is imperfect and might incorrectly identify innocent people as potential suspects. Those wrong matches could then be shared with other agencies, such as immigration enforcement, with far-reaching consequences.

“I am not sure Amazon has quite grappled with how their innovative technologies intersect with issues of privacy, liberty and government police power,” said Andrew Ferguson, a law professor at the University of the District of Columbia who studies how police use technology.

“The pushback they are getting comes from a failure to recognize that there is a fundamental difference between empowering the consumer

with information and empowering the government with information. The former enhances an individual's freedom and choice, the latter limits an individual's freedom and choice."

When law enforcement agencies are the customers, a company has an obligation to slow down, Ferguson said.

But Amazon is not slowing down. It says it has a duty to help police, defense and intelligence agencies.

"We believe our customers — including law enforcement agencies and other groups working to keep our communities safe — should have access to the best technology and believe that cloud services can materially benefit society," Amazon said in a statement.

'A game changer for law enforcement'

Police often say that they're not interested in which company sells a piece of technology, as long as the product is affordable and easy to use and helps keep people safe.

That is the philosophy in Chandler, a rapidly growing city outside Phoenix, where authorities noticed an increase in the number of residents who'd outfitted their homes with a new generation of internet-connected video cameras that monitor activity outside their front doors. The Chandler Police Department began looking for ways to make use of that growing network, and came across the Neighbors app.

The app is run by Ring — [bought by Amazon](#) for an estimated \$1 billion in early 2018 — which uses Neighbors to promote its popular line of doorbell cameras by encouraging members to share videos of suspicious activity. The platform includes a law enforcement portal that allows police departments [to post alerts and request video](#) from members who live near where a crime occurred. The portal can tell police agencies if anyone in a particular area recorded a Ring video at the time of a crime.

Chandler police got access to the portal by entering into an agreement

with Ring in which the company agreed to “seed” the partnership with a donation of 25 cameras to the department. The department gets another free camera for every 20 people who sign up [using a particular text code](#), Assistant Chief Jason Zdilla said. The city has given the free cameras away as door prizes to boost attendance at community meetings, he said.

The agreement — which appears to be a boilerplate document used in partnerships with police agencies around the country — also allows Ring to access Chandler Police Department’s “incidents/call logs.” Ring obtains that information through the city’s publicly available data portal and uses it to post alerts on Neighbors.

More than 20,000 Chandler residents are now on the Neighbors app, according to Zdilla. Police typically use the videos posted there to investigate property crimes, such as car break-ins and package thefts, but have also used the app to seek evidence of more serious crimes, including a fatal shooting. The department has an officer in each of its precincts assigned to search Neighbors for residents’ posts about potential crimes. But the department has also had to address false perceptions, stoked by the app and the publicity around it, that crime is on the rise.

Most videos obtained by police through Ring are voluntarily provided by homeowners, according to police and Amazon; the company declined to say how many subpoenas or court orders it has received for access to videos.

“This is a game changer for law enforcement because it basically is a virtual block-watch giving us the ability to communicate with a large number of people and the ability to ingest video from cameras in any case,” said Chandler police Cmdr. Edward Upshaw, who manages the department’s partnership with Ring. “It’s more information, more intelligence. We have a better sense of what’s going on in every single neighborhood.”

By embracing law enforcement in this way, Amazon has expanded Ring’s national network, from Fresno, California, to Cedar Rapids, Iowa, from

Houston to Norfolk, Virginia. Amazon declined to say how many police agencies have arrangements with Ring, but the nonprofit group Fight for the Future, which advocates against government surveillance, has [assembled a map](#) that identifies more than 50 of them.

The strategy fits into Amazon's aim to improve its home-delivery operations; the use of Ring cameras to catch people stealing packages from the front of homes has become a television news staple. Amazon has also provided materials to police to [conduct sting campaigns](#) aimed at luring thieves to snatch Amazon-labeled bait boxes from doorsteps under surveillance by Ring cameras. And the company has [filed a patent application](#) for outfitting Ring cameras with facial recognition.

Amazon's investment in this technology has prompted warnings that it is contributing to the creation of a runaway surveillance state fed by an overblown fear of crime.

[Read full story here...](#)