

Ring asks police not to tell public how its law enforcement backend works

Enlarge / Your local police might like to interest you in this product.

reader comments

168 with 93 posters participating

Share this story

Amazon's Ring line of consumer home surveillance products enjoys an extensive partnership with local police departments all over the country. Cops receive free product, extensive coaching, and pre-approved marketing lines, and Amazon gets access to your 911 data and gets to spread its network of security cameras all over the nation. According to a trio of new reports, though, the benefits to police go even further than was previously known—as long as they don't use the word "surveillance," that is.

Gizmodo on Monday published an email exchange between the chief of police in one New Jersey town and Ring showing that Ring edited out certain key terms of a draft press release before the town published it, as the company frequently does.

The town of Ewing, New Jersey, in March said it would be using Ring's Neighbors app. Neighbors does not require a Ring device to use; consumers who don't have footage to share can still view certain categories of crime reports in their area and contribute reports of their own, sort of like a Nextdoor on steroids.

Law enforcement has access to a companion portal that allows police to see an approximate map of active Ring cameras in a given area and request footage from them in the course of an investigation. The town also launched a subsidy program, giving up to 200 residents a \$100 discount on the purchase of Ring security products. Members of the police department also received \$50 discount vouchers for their own use.

The original draft press release, obtained by Gizmodo, showed that the town used one of Ring's pre-written press release templates and inserted a quote from the chief of police that read, in part, "Security cameras have been proven to be essential in deterring crime, and surveillance systems have assisted in closing cases that may have otherwise gone unsolved."

Ring approved a version with that sentence edited out, telling Ewing police the company avoids using the terms "surveillance" or "security cameras" because that might "confuse residents into thinking this program requires a Ring device or other system to participate or that it provides any sort of direct access to user devices and information."

If it quacks like a duck...

Police may not be allowed to use the words "surveillance" or "security cameras" in their marketing copy, but another pair of new reports highlights the significant surveillance capabilities Ring-branded security cameras can provide to law enforcement.

Local police departments have asked Ring to share "names, home addresses, and email addresses" of everyone who purchases a subsidized Ring device, Vice Motherboard reported yesterday, with some apparent success.

Email exchanges and other documents Motherboard obtained from several localities show that in at least three cities, Ring

had the capability to share a list of everyone who used a city subsidy to purchase a camera, theoretically to prevent homeowners from double-dipping.

In Arcadia, California, the company told city government that it would “provide the City with an address report for the products purchased in order to help the Arcadia Police Department track the location of Ring Video Doorbells and other Ring security camera equipment, and assess the level of community interest.”

“We have names of all the people who purchased if you want to block these people,” a Ring employee added in an email exchange with an Arcadia government employee. “We will match against names and emails of everyone who purchased at the event and prevent people from doubling up.”

A spokesperson for Arcadia told Motherboard that the city did not request a registry, nor have one in its possession. Ring also told Motherboard it “does not provide, and has never provided, resident information to law enforcement or cities participating in Ring’s subsidy match program” and said the statements Motherboard read were a “misrepresentation.”

Elsewhere in California, Motherboard found, Ring’s subsidy program contract with Rancho Palos Verdes includes a requirement that, for three years following completion of services, Ring must provide the city with “ledgers, books of accounts, invoices, vouchers, canceled checks, reports, studies,” as well as “all drawings, specifications, maps, designs, photographs, studies, surveys, data, notes, computer files, reports, records, documents and other materials” upon request. The company also told the city that it tracks the names, email addresses, and home addresses of everyone who buys a subsidized camera and places those addresses on a map to ensure they all fall within the city limits.

Ring told Motherboard that it both does and does not create

maps of consumers who buy subsidized cameras, confirming that it does so in order to check against the city limits but adds that it has “never created a map of everyone who used an online promo code as part of the subsidy program.”

A Ring representative contacted Ars after the publication of this story to dispute Motherboard’s reporting. The spokesperson said that Ring does not provide customer information to law enforcement partners, “period,” but also added that Ring device owners “submit their information knowing it will be used to verify their residency for the Ring subsidy program” and that the address verification process on the city end “allows Ring to cross reference residents who participate in a subsidy event with an official City record to determine eligibility” based on the agreement between Ring and the city.

Hush-hush

Ring device owners are often unclear on what information, specifically, police can see and how they can use it. That secrecy is entirely by design, CNET reports today, as Ring has a list of features its police partners are explicitly not supposed to share with the public.

Documents security researcher Shreyas Gandlur obtained through a FOIA request include a communication from Ring to police in Bensenville, Illinois, saying that “Neighbors Portal back-end features should not be shared with the public, including the law enforcement portal on desktop view, the heat map, sample video request emails, or the video request process itself as they often contain sensitive investigative information.”

CNET rounded up all of the information it could gather on those features from a combination of its own and others’ previous reporting, FOIA requests, and interviews with police. Among the features CNET describes in detail is the process through which police can request footage from local Ring

users.

For example, as part of an investigation into an auto theft, Bensenville police on July 11 sent a request for footage in a specific neighborhood taken in a 10-hour window between 8:00pm on July 9 and 6:00am on July 10. Users who received the request were presented with a big blue button reading, "Share your Ring videos now" or a smaller text option beneath to "check your Ring videos before sharing."

Users who decline to share footage through the app may have police showing up at their door asking them to share in person if online requests don't work out. Law enforcement can also go to Amazon directly with a valid legal demand and bypass the user's consent to access the footage entirely.

<https://arstechnica.com/?p=1555505>