Senator pushes Amazon for details about Ring “partnerships” with police

Enlarge / A Ring video doorbell mounted on a home.

reader comments

30 with 21 posters participating

Share this story

Amazon’s Ring line of video doorbells and home surveillance equipment is particularly popular with one key group: police. More than 400 law enforcement agencies around the country have partnered with Ring to use its apps and help market its security cameras to residents in the name of safer neighborhoods. As a dozen recent media reports have shown, however, the details about these partnerships and the privacy concerns they raise tend to be shrouded in secrecy and hard to learn.

Sen. Ed Markey (D-Mass.) is now among those who would like Amazon to explain what, exactly, Ring is up to. “The nature of Ring’s products and its partnerships with police departments raise serious privacy and civil liberties concerns,” Markey said in a letter (PDF) addressed to Amazon CEO Jeff Bezos.

“Although Amazon markets Ring as America’s ‘new neighborhood watch,’ the technology captures and stores video from millions of households and sweeps up footage of countless bystanders who may be unaware that they are being filmed,” Markey said in a statement. “I am particularly alarmed to learn that Ring is

pursuing facial-recognition technology with the potential to flag certain individuals as suspicious based on their biometric information."

Until very recently, Ring would not disclose how many of these partnerships it currently has. Following media pressure, however, the company said in late August it had 405 active agreements.

A growing list of concerns

Throughout the summer, reports from outlets including The Washington Post, Gizmodo, CNET, and Vice Motherboard have dug into the details of these agreements, which are rarely made public. The reports have found that Ring writes the press releases, social media posts, and talking points police departments use to encourage widespread Ring adoption. The company also asks police not to call its surveillance products "security cameras" or use the word "surveillance."

Concerns also abound about user privacy. Ring claims not to share lists of users or give maps pinpointing exact locations of cameras to police. In August, the company told Ars that participating agencies "must go through the Ring team when making a video request to customers," adding, "Customers can choose to opt out or decline any request, and law enforcement agencies have no visibility into which customers have received a request and which have opted out or declined."

But multiple reports have found evidence that Ring shared maps featuring active cameras with police in 2018, basically as a sales tactic to convince a police department to sign up for the partnership program by demonstrating how many cameras were already operating in its jurisdiction. Reports also found evidence that Ring collected data about purchasers which it then shared with police in order to cross-reference eligibility for subsidy programs or camera giveaways that police conduct, in partnership with Ring.

The company also gets access to 911 call data in some jurisdictions, which it uses to “curate” crime news for its Neighbors app. The app, while open to anyone, is optimized for Ring users, who can easily share footage from their doorbells through it. Police can also use their companion portal to send out a localized blast to Neighbors users requesting footage as part of an investigation. Although Ring now says it does not share data about users who decline to share their footage, at one point it gave cops a breakdown about how their requests were performing.

Late last year, the ACLU also flagged a patent application from Ring that would allow devices to ship with facial-recognition software, such as Amazon’s controversial Rekognition system. The patent would allow police or homeowners to flag certain faces as “suspicious.” If a suspicious face showed up on camera, police could then be dispatched to its location. Rekognition, however, is far from reliable and, like many other facial recognition services, is particularly likely to indicate false positives for people of color.

Clear answers?

Sen. Markey gave Ring until September 26 to answer questions that reporters and the general public have increasingly been trying to gain clarity on. Those inquiries relate not only to information requests but also to data retention and sharing policies, as well as other privacy concerns.

“How long has Ring prompted its users to share video footage with law enforcement?” Markey asked Ring, pushing for a “detailed timeline of when this sharing began and how, if at all, Ring has changed its policies” over time.

The letter asks Amazon to provide a list of all law enforcement agencies that have ever had or currently have access to Ring video, as well as a copy of a standard sharing

agreement. It also asks if Ring requires police departments to delete users’ footage after a certain period, if Ring requires police departments to handle footage in such a way as to minimize the risk of data breaches or leaks, and if Ring has any kind of language in those agreements either permitting or barring police from sharing footage they obtain with third parties.

Sen. Markey also expressed strong concern about the potential for Ring products to contribute to racial profiling and civil liberties violations, especially if Rekognition integration does become a feature. He asked the company to provide a timeline for when or if it plans to add such features as well as a list of criminal justice and civil liberties consultants it has consulted in its work.

https://arstechnica.com/?p=1562925