Citizen-on-Citizen Surveillance: All the Data that Amazon's Ring Cameras Collect on You

written by GEG | August 15, 2022

Amazon splashed out more than a billion dollars for Ring video doorbell in 2018, and its security products have exploded in popularity. Ring shares video and data with thousands of police departments, helping expand and normalize suburban surveillance. It is vulnerable to hacks. Privacy is violated as people can be monitored while walking through a neighborhood. Ring keeps detailed records, including every doorbell press and each motion the camera detects, and stores the information. Ring can record audio and conversations up to 20 feet away. Ring can also keep videos shared to its Neighbors' app and post videos of what is happening around the homes. Videos shared from security cameras and internet-connected doorbells have also become common on platforms like Facebook and TikTok, raking in millions of views.

If you walk through your local neighborhood—providing you live in a reasonably large town or city—you'll be caught on camera. Government CCTV cameras may record your stroll, but it is increasingly likely that you'll also be captured by one of your neighbors' security cameras or doorbells. It's even more likely that the camera will be made by Ring, the doorbell and security camera firm owned by Amazon.

Since Amazon splashed out more than a billion dollars for the company in 2018, Ring's security products have exploded in popularity. Ring has simultaneously drawn controversy for making deals (and sharing data) with thousands of police departments, helping expand

and normalize suburban surveillance, and falling to a string of hacks. While the cameras can provide homeowners with reassurance that their property is secure, critics say the systems also run the risk of reinforcing racism and racial profiling and eroding people's privacy.

Videos shared from security cameras and internet-connected doorbells have also become common on platforms like Facebook and TikTok, raking in millions of views. "Ring impacts everybody's privacy," says Matthew Guariglia, a policy analyst at the Electronic Frontier Foundation. "Most immediately, it impacts the people who walk down the streets every day, where the cameras are pointing out."

While Ring is far from the only maker of smart doorbells and cameras—Google's Nest line is another popular option—its connections to law enforcement have drawn the most criticism, as when it recently handed over data without warrants. So, what exactly does Ring collect and know about you?

What Ring Knows About You

Whenever you use any tech, it's collecting data about you. Spotify uses the data it collects to work out your mood, Slack knows how many messages you send. Ring's products are no different. Ring's privacy policy—running 2,400 words—and its terms of service detail what it collects about you and how it uses that information. In short: It's a lot.

Ring gets your name, phone number, email and postal address, and any other information you provide to it—such as payment information or your social media handles if you link your Ring account to Facebook, for instance. The company also gets information about your Wi-Fi network and its signal strength, and it knows you named your camera "Secret CIA Watchpoint," as well as all the other technical changes you make to your cameras or doorbells.

In March 2020, a BBC information request revealed that Ring keeps detailed records of people's doorbell activity. Every doorbell press was logged. Each motion the camera detected was stored. And details were saved every time someone zoomed in on footage on their phone. In just 129 days, 4906 actions were recorded. (Ring says it does not sell people's data.)

Ring can also collect the video and audio your camera records—the system doesn't record all the time, but it can be triggered when it senses movement. Ring says its cameras can detect movement "up to 155 degrees horizontally" and across distances of up to 25 feet. This means there's a good chance cameras can be triggered by people walking down the street or pick up conversations of passersby. According to tests by Consumer Reports, some Ring cameras can record audio from about 20 feet away.

Jolynn Dellinger, a senior lecturing fellow focusing on privacy and ethics at Duke University's school of law, says recording audio when someone is on the street is a "serious problem" for privacy and may change how people behave. "We operate with a sense of obscurity, even in public," Dellinger says. "We are in danger of increasing surveillance of everyday life in a way that is not consistent with either our expected views or really what's best for society." In October 2021, a British woman won a court

case that said her neighbor's Ring cameras, which overlooked her house and garden, broke data laws.

Ring's privacy policy says it can save videos of subscribers to its Ring Protect Plan, a paid service that provides an archive of 180 days of video and audio captured. The company says people can log in to the service to delete the videos, but the company may ultimately keep them anyway. "Deleted Content and Ring Protect Recordings may be stored by Ring in order to comply with certain legal obligations and are not retrievable without a valid court order," the privacy policy says.

Ring can also keep videos shared to its Neighbors' app—an app where people and law enforcement agencies can share alerts about "crimes" and post their videos of what is happening around the homes. (There are rules about what people are allowed to post.)

Ring's privacy policy and terms of service allow it to use all this information it collects in multiple ways. It lists 14 ways the company can use your data—from improving the service Ring provides and protecting against fraud to conducting consumer research and complying with legal requirements. Its privacy policy includes the ambiguous statement: "We also may use the personal information we collect about you in other ways for which we provide specific notice at the time of collection and obtain your consent if required by applicable law." Ring spokesperson Sarah Rall says this could apply if the company added features or use cases that are not already covered by its privacy policy. "We would provide additional notice or get permission as needed," Rall says.

While Ring's privacy policies apply to those who purchase its devices, people who are captured in footage or audio don't have a chance to agree to them. "Privacy, security, and customer control are foundational to Ring, and we take the protection of our customers' personal and account information seriously," Rall says.

Ultimately, you agree to give Ring permission to control the "content" you share—including audio and video—while you own the intellectual property to it. The company's terms of service say you give it an "unlimited, irrevocable, fee free and royalty-free, perpetual, worldwide right" to store, use, copy, or modify content you share through Neighbors or elsewhere online. (Audio recording can be turned off in Ring's settings.)

Read full article here…