Don't Buy Anyone a Ring Camera

gizmodo.com/dont-buy-anyone-a-ring-camera-1840070640

Illustration: Gizmodo

There's a chance you had never heard of Ring cameras before Amazon bought the company for as much as $1.8 billion last year. It's possible that Ring still wasn't on your radar earlier this year, when reports emerged that the home security giant had partnered with scores of police departments, funneling videos and user data in some dystopian effort to make a profit by fighting crime and eradicating privacy. But there's a good chance that you're going to see a Ring video doorbell on sale—possibly bundled with an Amazon Echo—this Black Friday.

Do not buy it. And definitely don't buy one for somebody else.

Ring is a troubled company. Last week a panel of five United States senators sent a letter to Amazon chief Jeff Bezos that expressed concern with Ring's struggles with information security and habit of sharing its users' videos not only with law enforcement but also with its Ukraine-based research team. The senators wanted to know how Ring encrypts user data (if at all) and how its internal security audits work. This is all happening after unsettling reports that Ring doorbells exposed users' home wi-fi passwords to hackers and that Ring employees spy on unwitting users.

These are troubles that any home security company could face. Information security is hard, and privacy can be tricky when your product is designed to make live video easily accessible to users on multiple devices. But the Ring story is somehow more sinister than that.

The story begins in 2011 when Jamie Siminoff invented a connected doorbell that could stream video to a phone. Siminoff called it Doorbot, and in 2013, mounted a successful crowdfunding campaign before appearing on *Shark Tank* to seek an additional $700,000 investment. The Shark Tank investors turned Siminoff down, but the inventor says the publicity sent sales through the roof. He renamed the company as Ring and later called the *Shark Tank* flop "extraordinary… worth millions."

It's not entirely clear when Siminoff decided to fight crime, but "to reduce crime in communities" has been the company's mission since at least 2014. That mission has evolved in curious ways. Following the early success of the Ring video doorbell, the company launched a whole suite of home security products, including motion sensors, indoor/outdoor cameras, an alarm system, and even smart lighting. In 2018, Ring also

released an app called Neighbors "to provide every neighbor with real-time, local crime and safety information." This neighborhood watch app has since been compared to Nextdoor and Citizen, two companies that have been mired in controversies of their own for years following accusations that they enable racial profiling and instill undue fear into communities. The problems with Neighbors are much worse.

The first problem is a technical one. Using the Ring app automatically enrolls you in Neighbors, and there's no way to opt-out. You don't have to post any frightening crime reports to the Neighbors feed, but if you want to use any Ring hardware, you have to be involved in the service. You can also sign up for Neighbors if you don't own any Ring products but are interested in policing your community.

That leads right into problem number two. Once you're enrolled in Neighbors—and remember, you have to be if you're using any Ring hardware—your videos or data could be shared with law enforcement agencies when requested. This sort of thing wouldn't be terribly different than any other tech company's practice of giving cops user data if presented with a warrant, but as Motherboard reported earlier this year, Ring has hundreds of once-secret partnerships with police forces around the country, partnerships that gave cops access to a "portal" where they could access video from Ring cameras in exchange for providing Ring with free advertising. The device's owners must give permission to share these videos with police, but it's also unclear how users might be compelled to share it.

These police partnerships were not only under wraps but also awfully deep. The Motherboard report reads, "In order to partner with Ring, police departments must also assign officers to Ring-specific roles that include a press coordinator, a social media manager, and a community relations coordinator." Gizmodo later reported that these press-facing roles were so involved that Ring actually edited press releases about Ring deals for police departments with whom it had contracts. As recently as April, one police memo showed, "over 225 law enforcement agencies" were engaged in these sorts of partnerships with Ring. In fact, everything that partner police organizations said about Ring was either written or approved by Ring.

The Ring surveillance saga is still unfolding. Just this week, The Intercept reported that Ring has been working on neighborhood "watch lists" based on artificial intelligence and facial recognition. We can only assume that Ring's law enforcement partners might gain access to these lists and possibly even funnel the data back into the fear machine that is the Neighbors app. Again, these cops can easily request access to videos from millions of Ring cameras, and according to Ring's privacy policy, Ring could compel users to share the footage based on "requests from government agencies." It's up to the users to trust that Ring will abide by its own privacy policy.

Does this sound like a company you should trust? It's under Congressional scrutiny for poor data security and problematic privacy practices. It's been engaged in dubious secret partnerships with police departments who can gain access to private home security camera feeds. Meanwhile, its corporate culture sounds weirdly militant. According to this revealing feature Los Angeles Times feature from 2017, Ring's founder Jamie Siminoff entertains some weird sort of militaristic fantasy at the office:

> He treats employees as confidants in war, bestowing them with dog-tag-style security badges inscribed with name, start date and title. He's honest about fear, retelling his nightmares to employees the morning after. World War II posters in the hallways emphasize the battle: "Loose Lips Sink Ring" and "Protect Our Neighborhoods."

Do you want to buy the cameras this company is selling? More importantly, do you want to gift one of these surveillance machines to a loved one?

Don't do it. Buy a Nest Hello doorbell. The hardware isn't perfect, but that company isn't feeding footage to the cops—that we know of. Better yet, buy a Logitech Circle 2 camera. You can review a whole day's worth of footage for free, and the company also probably isn't giving your personal data to cops.

Just steer clear of Ring.