Name: Julian Welge

Link: https://support.ring.com/hc/en-us/articles/360054941511-Understanding-Video-End-to-End-Encryption-E2EE-

Summary:

The home security service, Ring, is implementing end-to-end encryption for their video feeds for more private feeds of videos being captured. In doing this, multiple features intended for more seamless user surveillance of their property from their Ring devices will be disabled with end-to-end encryption.

What Ring features does Video E2EE disable?

Enabling Ring's Video E2EE will disable the following features for enrolled devices:

- Shared Users will not be able to view your videos.
- You will not be able to view encrypted videos on Ring.com, the Windows desktop app, the Mac desktop app, or the Rapid Ring app.
- You will not be able to use Live View from multiple mobile devices simultaneously.
- You will not be able to see camera previews on the Dashboard.
- You will not be able to share videos or links.
- You will not be able to use the Event Timeline.
- You will not be able to see Rich Event Notifications.
- You will not be able to watch Ring videos on Amazon Echo Show, FireTV, or FireTablet.
- You will not be able to watch encrypted videos on third-party devices.
- You will not be able to use Alexa Greetings.
- You will not be able to use Quick Replies.
- You will not be able to use Bird's Eye View.

Users will have the option to disable E2EE (end-to-end encryption) to get these features back if they so choose.

Why We Care:

Ring is making strides to secure their home surveillance services to essentially limit their services from being used as spyware, something that has become popular in use across the world, including use by government agencies infringing on peoples privacy rights such as what has happened in India with the Pegasus software.

What I believe Ring has realized is that the information that can be obtained from their devices without E2EE can actually make properties more vulnerable by providing deeper information of potential targets lives.

What is also concerning is allowing people to bypass using E2EE to keep their other convenient “security” features as this potentially allows a user who has not fully considered all of the potential consequences to disabling the E2EE capabilities.

One could also make the argument that this now infringes on the previous convenient security features and has brought the action of obtaining less-secure footage from Ring devices into the spotlight.