

Amazon's Ring Doorbells App Leaks Customers' Wi-Fi Username and Password. Report

By [Fight for the Future](#)

Global Research, November 13, 2019

[Fight for the Future](#) 7 November 2019

Region: [USA](#)

Theme: [Intelligence](#)

Today, Cyberscoop [reported](#) a major security vulnerability in Amazon's Ring doorbell app. Amazon's Ring doorbells, which have already raised significant privacy and civil liberties concerns, have now been shown to be deeply insecure, exposing users Wi-Fi passwords to hackers.

With this Wi-Fi information, hackers can access customers' personal home networks. It only gets scarier from there as hackers could use customer's webcams to spy on them and their children, gain access to their bank accounts, and retrieve personal information necessary for identity theft.

"This is a classic example of how more surveillance does not mean more safety," said Evan Greer, Deputy Director of Fight for the Future. "Amazon has consistently shown reckless disregard for privacy and civil liberties, but this is terrifying on a whole other level. Putting insecure cameras and listening devices around your home puts your family in danger. Congress should immediately investigate the threat posed by Amazon's rapidly spreading, for-profit surveillance dragnet."

Amazon's surveillance network doesn't only threaten our privacy and civil liberties, but our security as well. Meanwhile, millions of Americans continue to buy Ring products unaware of the dangers the technology and surveillance partnerships with police pose.

With over [550](#) partnerships across the country and millions of Americans potentially impacted, we need Congress to intervene. More than 10,000 people have already written their lawmakers [calling](#) on them to investigate Amazon's surveillance empire and their troubling partnerships with law enforcement.

*

Note to readers: please click the share buttons above or below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

The original source of this article is [Fight for the Future](#)

Copyright © [Fight for the Future](#), [Fight for the Future](#), 2019

[Comment on Global Research Articles on our Facebook page](#)

Become a Member of Global Research

Articles by: [Fight for the Future](#)

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca