February 29, 2024

Federal Communications Commission
Consumer and Governmental Affairs Bureau
Consumer Inquiries and Complaints Division
45 L Street NE
Washington, DC 20554

Federal Trade Commission
Bureau of Consumer Protection
600 Pennsylvania Avenue NW
Washington, DC 20580

Office of the California Attorney General
1300 "I" Street
Sacramento, CA 95814-2919

Re: Sale of insecure doorbell cameras on prominent e-commerce platforms

To Consumer Protection Authorities:

Consumer Reports[1] is writing to make you aware of significant security vulnerabilities uncovered in the course of our regular evaluation of internet-connected consumer products, in this case, wireless doorbell cameras. As laid out in more detail in the article we are publishing today,[2] these products can allow attackers to remotely access images generated by the cameras, allow a third-party to take over the doorbells in less than a minute, and send personally identifiable information over the internet in plain text. We have found these cameras operating under the name brands “Eken” and “Tuck” (and seemingly several other name brands as well) on major internet platforms including Amazon, Walmart, Temu, Sears, and Shein. In many cases, these doorbell cameras appeared among the top listing on search results for

[1] Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.

[2] Dan Wroclawski and Stacey Higginbotham, *These Video Doorbells Have Terrible Security. Amazon Sells Them Anyway*, Consumer Reports, (Feb. 29, 2024), https://www.consumerreports.org/home-garden/home-security-cameras/video-doorbells-sold-by-major-retailers-have-security-flaws-a2579288796/.

doorbell cameras, and were even affirmatively recommended by a platform in one case (being designed “Amazon’s Choice” on Amazon’s e-commerce platform).

First, all of the doorbell cameras we tested failed to even list FCC IDs on the product as required by law.[3] This is a rudimentary requirement for IoT products designed to ensure that the devices have been tested to ensure they do not cause harmful radio interference with other electronics or exceed safe radio-frequency limits for human health. The failure to meet this very threshold requirement was a potential warning sign that the products might fail short of other consumer protections as well, such as an obligation to design products with reasonable security.

And in fact, the cameras discussed in the CR story all demonstrated serious security vulnerabilities that could allow an attacker to access sensitive personal information, including still images and video feeds from the cameras. In our research, a CR researcher based in Yonkers, New York was able to access doorbell footage from test cameras installed by other CR employees without authentication or permission (CR employees consented to have their cameras hacked for this experiment).

The cameras all demonstrated significant security vulnerabilities in CR’s testing of the products: First, the doorbells expose your home IP address and WiFi network name to the internet without encryption, potentially opening your home network to online criminals. An attacker with physical access to the doorbell — such as an abusive ex-partner — also has the ability to press the doorbell for eight seconds to reset the doorbell, allowing them to then take control of the doorbell by pairing it to their own phone. This supersedes the owner’s access and if they save the serial number of the camera, they then have the ability to monitor the images created by the camera even if the doorbell owner takes control of the device back. The remote access to images from the device, persists without authentication or notice to the device’s owner.

For nearly thirty years, the Federal Trade Commission has enforced Section 5 of the FTC Act to prohibit companies from deploying products and services without reasonable security safeguards to protect user’s personal data from outside attack.[4] The behaviors described above leave consumers’ devices and recordings accessible to others and could be easily prevented by cost-effective, industry-standard practices such as encrypting the data transmitted by the device both locally and in the cloud, as well as by requiring authentication before allowing someone to access images stored in the cloud.

---

[3] GENERAL GUIDELINES FOR LABELING AND OTHER INFORMATION REQUIRED TO BE PROVIDED TO USERS, Fed. Communications Comm’n, (Nov. 2, 2023), https://apps.fcc.gov/kdb/GetAttachment.html?id=zxVuCJtYn65mLwFupyGdmw%3D%3D&desc=784748%20D01%20general%20labeling%20and%20notification%20v09r02&tracking_number=27980

[4] *See* Press Release, *BJ's Wholesale Club Settles FTC Charges*, (Jun. 16, 2005), Fed. Trade Comm’n., https://www.ftc.gov/news-events/news/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges; Press Release, *DSW Inc. Settles FTC Charges*, (Dec. 1, 2005), https://www.ftc.gov/news-events/news/press-releases/2005/12/dsw-inc-settles-ftc-charges.

In addition, these doorbells may also violate new state-level laws explicitly mandating reasonable security practices, including California's first-in-the-nation IoT cybersecurity law, SB 327. That law specifically regulates connected devices such as the doorbells at issue here and provides that:

> a) A manufacturer of a connected device shall equip the device with a reasonable security feature or features that are all of the following:
>
> (1) Appropriate to the nature and function of the device.
>
> (2) Appropriate to the information it may collect, contain, or transmit.
>
> (3) Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.[5]

By engaging in the behaviors described above, it is likely that the device manufacturers have not equipped those devices with features that meet the criteria laid out in the statute.

Finally, in considering interventions to address the sale of insecure products such as the ones described here, we recommend you look not just to the manufacturers selling these devices but also the platforms that distribute and profit from them. As discussed in the article, these cameras were included within the top listings for search results on many of these platforms, and in at least one case was affirmatively recommended to consumers. While one platform responded to our outreach and removed the doorbell cameras from product listings, others, including Amazon, Shien, and Sears, took no action or refused to acknowledge our outreach altogether.

Section 5 and state-level consumer protection laws such as California Unfair Practices Act give regulators broad authority to pursue unfair business practices that harm consumers. As discussed above in the security context, this includes holding platforms responsible for failing to take reasonable steps to remediate the harms caused by malicious outside actors. And even outside of the data security context, the FTC has taken action against platforms that failed to address fraudulent practices conducted by third-parties by taking reasonable interventions.[6]

---

[5] California Code, Civil Code, CIV § 1798.91.05, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.

[6] *See*, *e.g.*, Press Release, *FTC Sues Walmart for Facilitating Money Transfer Fraud That Fleeced Customers Out of Hundreds of Millions*, Fed. Trade Comm'n, (Jun. 28, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-sues-walmart-facilitating-money-transfer-fraud-fleeced-customers-out-hundreds-millions; Press Release, *U.S. Circuit Court Finds Operator of Affiliate Marketing Network Responsible for Deceptive Third-Party Claims Made for LeanSpa Weight-loss Supplement*, Fed. Trade Comm'n, (Oct. 4, 2016), https://www.ftc.gov/news-events/news/press-releases/2016/10/us-circuit-court-finds-operator-affiliate-marketing-network-responsible-deceptive-third-party-claims. Press Release, *Court Orders Permanent Halt to Illegal Qchex Check Processing Operation Court Finds Qchex Unfair Practices Created a Dinner Bell for FraudstersOperators to Give Up All Their Ill-Gotten Gains*, Fed. Trade Comm'n, (Feb. 9, 2009), https://www.ftc.gov/news-events/news/press-releases/2009/02/court-orders-permanent-halt-illegal-qchex-check-processing-operation-court-finds-qchex-unfair.

In this case, platforms' failure to conduct basic due diligence of the products sold on its platform is likely to lead to significant consumer harm that is not reasonably avoidable by consumers and is not outweighed by benefits to consumers or competition.[7] This is especially the case when a platform affirmatively recommends the product to consumers (such as labeling the product "Amazon's Choice") or fails to take steps to address even when provided notice of failings through the mechanisms specifically set up for that purpose. While it is possible the platforms may assert Section 230 immunity for their role in facilitating the purchase of third-party goods, Section 5 liability does not depend on deeming platforms to be the "speaker" of the content provided by third-party merchants; instead, it holds the platforms responsible for their own content in facilitating transactions and failing to take remedial steps to address the harms caused by those transactions. It is important to note that the premise that Section 230 insulates e-commerce platforms from the harms caused by third-party sellers has been rejected by several courts.[8]

Thank you for your consideration of these findings and recommendations. If there is any additional information we could provide to you with regard to this investigation, please do not hesitate to reach out to us at stacey.higginbotham.consultant@consumer.org.

Sincerely,

Stacey Higginbotham
Policy Fellow
Consumer Reports

Justin Brookman
Director of Technology Policy
Consumer Reports

[7] 15 U.S.C. § 45(n).
[8] *See*, *e.g.*, *Loomis v. Amazon.com LLC* (2021) 63 Cal.App.5th 466; *Bolger v. Amazon.com LLC* (2020), 53 Cal.App.5th 431; *Oberdorf v. Amazon.com Inc.*, 930 F.3d 136, 154 (3d Cir.), reh'g en banc granted, opinion vacated, 936 F.3d 182 (3d Cir. 2019).