January 13, 2020

To Whom It May Concern:

In response to multiple reports of hacks and unauthorized access of smart cameras and doorbells, Consumer Reports writes to urge your company to raise the standard of security for your connected camera, doorbell, or security system. We request clarification on the steps you are taking to prevent hacks and unauthorized access to these cameras and the systems that underlie them.

We also want makers of connected devices to know that CR's ratings will continue to change to reflect the stronger data security and privacy practices we believe are essential for consumer protection, which could impact a product's eligibility for recommendation.

Connected devices such as cameras are increasingly being used in the private sphere of the home and collect highly sensitive information including voice and visual recordings of the home and the area immediately around a private residence. However, as multiple reports of connected camera hacking and incidents of unauthorized access have shown, many of these products are built without adequate security. Attackers have openly viewed home security systems and baby monitor feeds, and have even spoken with residents, including young children.

All people have an inherent right to privacy—especially within their own homes. This right to privacy at home is protected in the US Constitution and is clearly reflected in consumer preferences regarding connected products used at home. For example, although smart home systems are on the rise, consumers are more concerned with privacy than cost.[1] In addition, although consumers want to feel secure at home, the majority of users who already own a security system (72 percent) are worried that their home security companies will invade their privacy and almost a fourth of users (23 percent) deactivate the system completely when guests are over.[2] Even a senior vice president at Google warned owners of smart speakers, devices that collect sensitive audio data to turn off their speakers when a guest visits.

And these privacy concerns are indeed warranted. The risks have been known and documented for years. As early as 2015, the Federal Bureau of Investigation warned consumers that the connected

[1] Rob Marvin, *Privacy Tops List of Consumer Smart Home Concerns*, PC MAG (Mar. 4, 4019, 5:00 AM), https://www.pcmag.com/news/366783/privacy-tops-list-of-consumer-smart-home-concerns.

[2] Nicholas Shields, *New Survey Shows Consumers Are Wary of Smart Home Devices Invading Their Privacy*, BUS. INSIDER (Apr. 26, 2018, 4:44 PM), https://www.businessinsider.com/survey-says-consumers-have-privacy-concerns-with-smart-home-devices-2018-4.

products in the home could make users vulnerable to exploitation, specifically mentioning "Security systems, such as security alarms or Wi-Fi cameras, including video monitors used in nursery and daycare settings." Yet the number of reported incidents of hacked cameras being used to harass and scare people in December 2019 alone are numerous:

- A woman reported that a man had hacked her camera, which she only learned when the man started to harass the woman through the camera in her bedroom.
- A stranger also hacked a family's camera to spew racial slurs at the family.
- A hacker demanded a man pay a ransom in bitcoin through his connected camera.
- A woman was awoken by someone shouting "wake up" through a connected camera located in her bedroom.
- A family learned that their home cameras had been hacked only when a stranger's voice yelled through the camera to "Come here. Come here."

These stories represent only five of the at least 17 reported incidents in the US in December, according to a search conducted by Consumer Reports. The hacking of connected cameras has become so frequent that there is a podcast telling people how to hack one company's products.[3]

In light of consumer concerns and this long history of connected camera hacking, Consumer Reports is urging your company to implement stronger security measures to adequately protect consumers and their privacy. These measures may include but are not limited to:

- automatic firmware/software updates enabled by default;
- protection against credential stuffing and reuse;
- require multifactor authentication and captchas in the authentication system;
- email notifications for users when a login occurs from a new device or a new IP address;
- require users to sign back in after changing a password;
- confirm with the user when the credentials have been changed;
- password creation rules that require more secure passwords, and compatibility with password managers;
- increased protection against brute-force dictionary attacks by rate-limiting login attempts; and
- inclusion of a visible indicator (e.g., a prominent LED light) when cameras are active.

We are interested in knowing which of these security measures you have implemented for your connected products and what additional security measures you plan to implement in the future (and by what date). To that end, we request a response by **Monday, January 27th, 2020**.

[3] Joseph Cox & Jason Koebler, *Inside the Podcast that Hacks Ring Camera Owners Live on Air*, VICE (Dec. 12, 2019), https://www.vice.com/amp/en_us/article/z3bbq4/podcast-livestreams-hacked-ring-cameras-nulledcast?.

We also welcome a conversation about what the minimum security standards should be for connected cameras and doorbells.

Please direct your response to Katie McInnis.

Sincerely,

Katie McInnis
Policy Counsel
Consumer Reports
1101 17th Street NW, Suite 500
Washington, DC 20036