MARK R. WARNER
VIRGINIA

United States Senate

WASHINGTON, DC 20510–4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

May 22, 2017

The Honorable Maureen K. Ohlhausen
Acting Chairwoman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20530

Dear Acting Chairwoman Ohlhausen,

I am writing to express my continued and growing concern regarding children's privacy amid recent media reports further highlighting security vulnerabilities in a wide array of connected products directed at children. While I remain grateful for the work the Federal Trade Commission (hereafter "FTC") has done to protect America's children, I worry that protections for children are not keeping pace with consumer and technology trends shaping the market for these products. In particular, recent events have illustrated that in addition to security concerns with the devices themselves, new data-intensive functionalities of these devices necessitate attention to the manner in which vendors transmit and store user data collected by these devices. Reports of your statements casting these risks as merely speculative – and dismissing consumer harms that don't pose "monetary injury or unwarranted health and safety risks" – only deepen my concerns.[1]

In May 2016, I sent a letter to then Chairwoman Edith Ramirez in which I noted the "increasing prevalence of connectivity and data processing abilities in children's toys and other household products." In that letter, I raised a number of concerns regarding the security of internet-connected devices, known collectively as the Internet of Things (IoT). In particular, I was alarmed by the growth of connected devices marketed toward children, such as internet-connected dolls and toy cars, given security vulnerabilities researchers have identified in a number of these products. Recent media reports have raised additional concerns not only about the security of connected devices but also about the remotely stored data generated from these devices. This latter point is notable given the data minimization requirements of the Children's Online Privacy Protection Act (COPPA), prohibiting service providers from retaining collected personal information longer than is necessary to fulfill the purpose for which the information was originally collected.

A timely example of the insecurity in some of these IoT devices is CloudPets, a product line manufactured by Spiral Toys and marketed as 'a message you can hug,' which according to

[1] Maureen Ohlhausen, *ABA 2017 Consumer Protection Conference: Opening Keynote*, Federal Trade Commission (February 2, 2017), https://www.ftc.gov/system/files/documents/public_statements/1069803/mko_aba_consumer_protection_conference.pdf.

multiple media reports was storing personal data in an insecure, public-facing online database.[2] Ignoring the most basic elements of responsible data management, CloudPets reportedly exposed over 800,000 customer credentials and more than two million voice recordings sent between parents and children.[3] Additional reports have subsequently raised questions about security at the device level, with individuals able to hack CloudPets' toys and remotely control the devices, including the microphone, as long as they are within Bluetooth range.[4] This one example demonstrates the importance of better incorporating security at the device level, on servers holding data collected by these devices, and across communications links.

Following the massive Distributed Denial of Service (DDoS) attack in October 2016 that flooded particular websites, web-hosting servers, and internet infrastructure providers with debilitating levels of network traffic from insecure IoT devices, I sent a letter to your agency in which I asked what the FTC would do to take harmful devices out of the stream of commerce. The agency responded that, among other things, the FTC has "urged companies to continuously monitor the threat landscape and update and release security patches throughout the lifecycle of their devices."

Researchers have determined that in many cases IoT devices are, by design, not patchable. As I noted in my October letter, a lack of market incentives to design devices with security in mind or to provide ongoing support has allowed manufacturers to flood the market with cheap, insecure devices. In March, however, you seemed to downplay the existence of these risks, suggesting that "We don't know if that risk [from insecure IoT devices] will materialize," and contending that *if* it did, industry could sufficiently address the problem, obviating the need for FTC action.

In fact, there are reports that indicate that security researchers made repeated attempts to get in touch with CloudPets regarding the vulnerabilities they found, but were unable to reach company representatives. Companies should welcome feedback from experts and establish coordinated disclosure programs, where researchers can alert vendors of important vulnerabilities. While I understand some companies may be vary of establishing such programs, ignoring security researchers or waiting for notification from an agency like the FTC presents unnecessary risks to consumers by allowing vulnerabilities to go unfixed.

While instituting coordinated vulnerability disclosure programs would certainly help improve device and data security, more drastic actions may be necessary to address vulnerabilities in the deployed base of products purchased by consumers. As you may be aware, other countries have taken steps to remove insecure internet-connected devices from the marketplace or warn parents about the dangers of such toys. On February 17, 2017, Germany's Bundesnetzagentur or Federal Network Agency, an entity responsible for regulating energy, telecommunications, post, and rail networks, pulled the children's doll "My Friend Cayla" off the market due to concerns that the

---

[2] *See* Lee Matthews, *The Latest Privacy Nightmare for Parents: Data Leaks from Smart Toys*, Forbes (February 27, 2017), https://www.forbes.com/sites/leemathews/2017/02/28/cloudpets-data-leak-is-a-privacy-nightmare-for-parents-and-kids/#9a394e3b0bfa.

[3] *See* Anthony Cuthbertson, *Internet-Connected Teddy Bear Leaks 2 Million Voice Recordings of Parents and Children,* Newsweek (February 28, 2017), http://www.newsweek.com/internet-connected-teddy-bear-leaks-2-million-voice-recordings-parents-and-561969?rx=us.

[4] *See* Gabriela Vatu, *CloudPets Nightmare Part 2:Toys Can Be Hacked via Bluetooth,* Softpedia (March 1, 2017), http://news.softpedia.com/news/cloudpets-nightmare-part-2-toys-can-be-hacked-via-bluetooth-513449.shtml.

device could be used for unauthorized surveillance.[5] The FTC received a complaint from privacy advocates in December 2016 regarding "My Friend Cayla," but has not taken concrete action as of May 22, 2017.[6]

Given these recent developments, I have a number of questions regarding the FTC's actions to protect children's privacy and respectfully request responses within four weeks of receipt.

1. While the Children's Online Privacy Protection Act (COPPA) has requirements regarding the security of children's data, hacks of companies like CloudPets and VTech have shown that children's data is still vulnerable. Do COPPA's data security – including retention and data minimization – standards need to be updated? Are companies ignoring COPPA requirements, or are COPPA requirements not keeping pace with developments in data security and cyber security best practices?

2. Does the FTC need additional authority from Congress to regulate the remote storage of data by operators or by third parties who store and handle children's personal information?

3. In the case of a civil enforcement action related to a violation of either Section 5 or COPPA, does the FTC's injunctive authority extend to requiring defendants to recall insecure products designed for, marketed, and sold to U.S.-based consumers? Under what circumstances might the FTC require a 'buy-back' for insecure products, as it did in a recent Section 5 case involving an automaker's deceptive marketing?

4. Has the FTC been in contact with CloudPets or its parent company Spiral Toys? If not, why has the FTC not been in contact?

5. What guidance has the FTC given to Spiral Toys or CloudPets? Has the FTC issued guidance or considered issuing guidance to consumers who bought products from Spiral Toys or CloudPets whose data has been compromised?

6. As mentioned above, privacy advocates filed a complaint with the FTC in December 2016 regarding "My Friend Cayla." Has the FTC taken any action with respect to "My Friend Cayla" or other products manufactured by Genesis Toys?

---

[5] Bundesnetzagentur Press Office, *Bundesnetzagentur removes children's doll "Cayla" from the market,* Bundesnetzagentur (February 17, 2017), https://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/BNetzA/PressSection/PressReleases/2017/17022017_cayla.pdf?__blob=publicationFile&v=2.

[6] Complaint and Request for Investigation, Injunction, and Other Relief by the Electronic Privacy and Information Center, *In the Matter of Genesis Toys and Nuance Communications,* Federal Trade Commission (December 6, 2016), https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf

7. Insecurities associated with IoT devices have been widely known for a number of years. On what basis are you concluding that these risks have yet to materialize, or that market solutions have successfully addressed these harms?

I thank you for your continuing cooperation in protecting the privacy and safety of children across the United States. I hope that we can work together to ensure proper oversight of this issue.

Sincerely,

Mark R Warner

MARK R. WARNER
United States Senator