June 2, 2016

Travis Hall,
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Attn: IOT RFC2016
Washington, DC 20230

Re: Common Sense Kids Action Comments on The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things

Common Sense Kids Action, the advocacy arm of Common Sense Media (collectively, Common Sense) is pleased to submit these comments in response to the request for public comment by the National Telecommunications and Information Administration (NTIA) regarding the Internet of Things. Common Sense is a national, independent, nonpartisan voice for America's children, working to ensure that every child has the opportunity to thrive in the 21st century. We appreciate the NTIA's interest in and attention to this growing field.

The Internet of Things (IoT) and smart devices can bring many conveniences—and sometimes a sense of wonder—to daily life. IoT also raises old privacy and educational concerns and surfaces many new ones. Common Sense is particularly concerned about IoT's privacy implications for families and children, as innovative toy and device makers often seem less focused on privacy and security than on developing the newest hit gadget. Common Sense is also concerned about the implications these devices have for children's broader education.

IoT Brings Internet Tracking to Babies

IoT devices, unlike traditional Internet-connected devices, are often screen-less and button-less. They are designed to be used intuitively, played with, and worn on the body. In short, even a very young child can operate many of them. And many do. Indeed, these devices seem designed for younger and younger audiences, including babies. In recent years, the following products have been announced:

- A bootie that monitors baby's breathing and connects to a smartphone.[1]
- Smart bottles that measure consumption.[2]
- A Fitbit-like device for kids that comes with a pet pal.[3]

[1] *Owlet: Rest Assured;* http://www.owletcare.com.
[2] Bonnie Cha, *Smart Baby Bottles, 3-D*, (Jan. 9th, 2015); http://www.recode.net/2015/1/9/11557630/smart-baby-bottles-3-d-food-printers-and-other-ces-oddities.

2200 Pennsylvania Ave., NW,
4th Floor East
Washington, D.C. 20037
(202) 350-9992

650 Townsend Street
San Francisco, CA 94103
(415) 863-0600

- Internet-enabled baby thermometers.[4]
- Geolocation watch phones for toddlers and preschoolers.[5]

Talking dolls and toys, in addition to smart thermostats and other gadgets, are increasingly present in families' homes. They are the next frontier after mobile, which has already gobbled up the attention of a younger audience (and their parents) and has been used by virtually every American child.[6]

Unfortunately, little is understood about risks of IoT. What is known, particularly regarding privacy and security, is not encouraging. Companies appear to be making privacy and security an afterthought. And notices and terms of service are often buried on a website, unconnected from the physical devices. Meanwhile, claims of educational value—which may have little basis—are front and center to attract parents.

Children's IoT Devices Are Insecure, Leaving Kids and Families Vulnerable

Anyone even passingly familiar with hackable home devices has been aware for some time of how insecure many Wi-Fi baby monitors are, with the FTC finding insecure devices in use in 2012[7] and continuing to the present day.[8] Unfortunately, this is just the tip of the iceberg for hackable kids' devices. Last year, just before the holiday shopping season, popular game and toy manufacturer VTech suffered a massive data breach. Six million children, and five million parents, had their information hacked.[9] As explained by Bill Fitzgerald, Director of Common Sense's Privacy Initiative, "The toy manufacturer had failed to use basic security measures to protect most of this data, and when they attempted to encrypt data, they used a method that has been obsolete for years."[10] Data exposed in the breach included names, dates of birth, password recovery questions and answers, genders, pictures of parents and children, audio recordings of children, and chat logs between parents and children, including intimate moments such as, "Roses are red vilets [sic] are blue and I love you. Mommy and daddy."[11] As if this were not disappointing enough, VTech's initial response appeared to be to disclaim responsibility in small print—it inserted language buried into its terms of service on its Learning Lodge website that customers acknowledged information sent and received may not be secure.[12]

---

[3] *LeapBand;* http://www.leapfrog.com/en-us/products/leapband.
[4] *Temp Traq;* https://www.temptraq.com.
[5] *Filip;* http://www.myfilip.com.
[6] Over three-quarters of children under 2 use a mobile device every day. *Exposure and Use of Mobile Devices by Young Children,* (Oct. 2015); http://pediatrics.aappublications.org/content/early/2015/10/28/peds.2015-2151.
[7] *Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy,* (Sep. 4, 2013); https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles.
[8] Seena Gressin, *Is Your Baby Monitor Secure?*, (Jan. 19, 2016); https://www.consumer.ftc.gov/blog/your-baby-monitor-secure.
[9] *See, e.g.*, Bill Fitzgerald, *Privacy, Parenting, and the VTech Breach,* (Dec. 3, 2015), https://www.commonsensemedia.org/blog/privacy-parenting-and-the-vtech-breach.
[10] *Id.*
[11] *Id.*
[12] *See, e.g., VTech: We Are Not Liable If We Fail to Protect Your Data, EFF: Oh Yes You Are!,* (March 9, 2016); https://www.eff.org/deeplinks/2016/03/vtech-we-are-not-liable-if-we-fail-protect-your-data-eff-oh-yes-you-are.

Around the same time, news outlets revealed that Hello Barbie—a talking and listening device designed to converse with young children, and long the source of concern among privacy and children's advocates, including Common Sense[13] – was hackable and could be used to spy on the very same children with whom Barbie was "playing."[14] The Guardian reported that the toy "can easily be hacked to turn it into a surveillance device for spying on children and listening into conversations without the owner's knowledge."[15] This spring, the makers of Hello Barbie are doubling down on listening-device equipped children's toys: Hello Barbie has her own Dream House.[16] As noted in the press, "Instead of addressing the privacy concerns raised by the original Hello Barbie, Mattel has instead come out with a sprawling mansion for the doll that also listens and responds to children's requests using a Wi-Fi connection to the Internet."[17] The Dream House appears to function like Amazon's Echo or Google's Home,[18] both of which are advertised for an entire household, including kids,[19] and which may be attractive to children or teens eager for the latest gadget. Such interactive listening devices, whether explicitly aimed at young kids or aimed at families more generally, seem poised to grow exponentially.

These devices, many of which lack built-in privacy and security protections, raise numerous policy concerns. Kids are already more susceptible to identity theft than adults,[20] and such devices raise the risk that even more kids will be victims. They raise the risk of children's intimate conversations with their toys being used to sell more products to kids or their parents, or being used to channel children into certain pathways or noted as aggressive, violent, or some other attribute at ever earlier ages. A child's geolocation could be tracked by an unintended party. Babies' eating habits, temperature, or sleeping habits may be used to market products to already over-sold and sleep-deprived new parents, or, a toddler's activity level could be used for

---

[13] *See, e.g,* Evie Nagy, *After the Fracas Over Hello Barbie, ToyTalk Responds to its Critics, (*May 23, 2015)*;* http://www.fastcompany.com/3045676/tech-forecast/after-the-fracas-over-hello-barbie-toytalk-responds-to-its-critics; Sarah Halzack, *Privacy Advocates Try to Keep 'Creepy,' 'Eavesdropping' Hello Barbie from Hitting Shelves*, (March 11, 2015); http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/11/privacy-advocates-try-to-keep-creepy-eavesdropping-hello-barbie-from-hitting-shelves/.

[14] Samuel Gibbs, *Hackers Can Hijack Wi-Fi Hello Barbie to Spy on Your Children,* (Nov. 26, 2015), https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children.

[15] *Id*.

[16] Andrew Liszewski, *Barbie Now Has an Entire Smart Dream House That Responds to Kids' Voice Commands,* (Feb. 13, 2016)*;* http://toyland.gizmodo.com/barbie-now-has-an-entire-smart-dream-house-that-respond-1758964921.

[17] Andrew Liszewski, *All the Coolest Stuff From Toy Fair 2016* (Feb. 16, 2016); http://toyland.gizmodo.com/all-the-coolest-stuff-from-toy-fair-2016-1759253744.

[18] *See, e.g.,* Michael Liedtke, *Google Echoes Amazon's Echo, Opens New Virtual-Reality Door,* (May 18, 2016); https://www.washingtonpost.com/business/technology/expect-virtual-reality-artificial-intelligence-from-google/2016/05/18/c0b99ac0-1cad-11e6-82c2-a7dcb313287d_story.html.

[19] Advocates have raised concerns about the devices' marketing materials, which feature young children. Mark Harris, *Virtual Assistants such as Amazon's Echo Break US Child Privacy Law, Experts Say,* (May 26, 2016), https://www.theguardian.com/technology/2016/may/26/amazon-echo-virtual-assistant-child-privacy-law.

[20] Richard Power, *Child Identity Theft: New Evidence Indicates Identity Thieves are Targeting Children for Unused Social Security Numbers*; https://www.cylab.cmu.edu/files/pdfs/reports/2011/child-identity-theft.pdf; *see also* Ariel Fox Johnson, *Giving California Kids a New Way to Fight Identity Theft*, (May 3, 2016); https://www.commonsensemedia.org/kids-action/blog/giving-california-kids-a-new-way-to-fight-identity-theft.

future health or medical diagnoses by black box algorithms. Insurers could make pricing or eligibility decisions, entirely unbeknownst to families. The device makers often do not know why they are collecting the data, and for what purpose,[21] and therefore we as consumers cannot know either. Furthermore, most of these concerns become confounded when you consider that the devices are not just themselves monitoring individuals, but oftentimes now communicating with other devices in the home too, as cross-device tracking becomes more the norm.[22] The amount of information available for the taking from a nursery, for example, is staggering.

The Educational Value of IoT Is Not Well Understood

As the next big thing, connected toys raise policy concerns outside of the privacy and security sphere as well. The educational value of toys—and many other products—is often exaggerated and difficult to ascertain. While some IoT devices appear to show great promise, by, for example, encouraging *more* adult-children interaction,[23] which is supported by research,[24] many devices and apps billed as educational may in reality fail to advance children's growth or have no basis upon which to make "educational" claims.[25] Educational promises are difficult to assess, and all the more so when they come attached to fancy new technology. And this is to say nothing of what the Internet of Things may do to a young person's growing understanding of the world. In a Pew Report about IoT, one pioneering Internet sociologist and educator questioned, "what child will be able to know that a doorknob that recognizes their faces doesn't also know many other things?"[26] It is a brave new world for both kids and adults.

Kids' IoT Requires Research and Guidance, Including Comprehensive Regulations

The NTIA and others with jurisdiction in this space, such as Congress and the Federal Trade Commission, should study the implications of IoT for children and teens. What sort of notice is appropriate and necessary for screen-less IoT toys, which may be sold on shelves or online, and where should such notice be placed? How will companies ensure that parents understand the full surveillance power of the toys and devices they are purchasing for their

---

[21] Following the VTech revelations, Sens. Markey and Barton sent a letter to VTech that included such pertinent questions as, "For each type of information collected by the company, please specify whether that information is required to make the toy or product function properly…. If the information is not required to make the toy or product properly function, please explain why the information is still collected." http://www.markey.senate.gov/imo/media/doc/2015-12-02-VTECH-Letter-Markey-Barton.pdf. As of May 19, VTech had not publicly responded.

[22] Ariel Fox Johnson and Bill Fitzgerald, *Comments on Cross Device Tracking*, (Dec. 17, 2015); https://www.commonsensemedia.org/about-us/news/press-releases/common-sense-files-comments-to-federal-trade-commission-on-cross-device.

[23] *See, e.g., Starling*; https://www.versame.com.

[24] Maya Shankar, *Empowering Our Children by Bridging the World Gap*, (June 25, 2014); https://www.whitehouse.gov/blog/2014/06/25/empowering-our-children-bridging-word-gap.

[25] *Educational App or Digital Candy? Helping Parents Choose Quality Apps for Kids,* (May 6, 2015)*;* http://www.psychologicalscience.org/index.php/news/releases/educational-app-or-digital-candy-helping-parents-choose-quality-apps-for-kids.html; Corey Turner, *The Trouble With Talking Toys*, (Jan. 11, 2016); http://www.npr.org/sections/ed/2016/01/11/462264537/the-trouble-with-talking-toys.

[26] Howard Rheingold, featured in *The Internet of Things Will Thrive by 2025*, (May 14, 2014); http://www.pewinternet.org/2014/05/14/internet-of-things/.

children, and how can companies help parents make smart choices (like using secure passwords) to help protect themselves and their families? How can parents understand the educational benefits and limitations of the devices they are purchasing? How should children approach such devices and how can they understand the capabilities and unforeseen consequences that may come from using such devices? How can companies make accurate and non-misleading claims about the educational nature of their products? How can we encourage toymakers to build in privacy and security by design, and not in response to a breach? How should companies appropriately respond to breaches?

In addition, strong and comprehensive laws and regulations will help provide clear guidance to companies operating in this space and peace of mind for consumers. Such laws and regulations may include a COPPA update to explicitly reflect IoT (including, for example, when IoT devices are deemed child-directed), just as past updates have acknowledged mobile.

Further, while a multistakeholder approach may be appropriate for research and inquiry into IoT, it is not the best way to create strong guidelines and regulations. As seen with the recent NTIA Facial Recognition Proceeding, which Common Sense and other consumer advocates left in protest,[27] even with the best intentions and efforts of NTIA and its staff, industry will abuse such proceedings and make it impossible for consumers—including kids and families—to be better off. Rather, after studying the matter, the NTIA and others charged with regulating this space and protecting the public should craft appropriate guidelines, laws, and regulations.

Common Sense looks forward to working with the NTIA and other policymakers and stakeholders on this important issue.

Respectfully submitted,

Ariel Fox Johnson
Senior Policy Counsel, Privacy and Consumer Affairs
Common Sense Kids Action

[27] Privacy Advocates Statement on NTIA Face Recognition Process; https://www.eff.org/document/privacy-advocates-statement-ntia-face-recognition-process; *see also* Alvaro M. Bedoya, *Why I Walked Out of Facial Recognition Negotiations;* http://www.slate.com/articles/technology/future_tense/2015/06/facial_recognition_privacy_talks_why_i_walked_out.html.