epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

Comments of the
ELECTRONIC PRIVACY INFORMATION CENTER
to the
European Commission

Evaluation of the Toy Safety Directive (2009/48/EC)

December 12, 2018

By notice published September 9, 2018, the European Commission ("the Commission") requests public comment on the efficacy of the Toy Safety Directive (2009/48/EC) in protecting children's health and safety by setting harmonized safety requirements for toys distributed within the European Union.[1]

Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits the following comments to (1) highlight the serious safety risks posed by Internet-connected toys and (2) urge the Commission to develop safety guidelines for connected toys.

EPIC is a public interest research center in Washington D.C. that was established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] For over twenty years, EPIC has been committed to protecting children's privacy. EPIC helped draft and enact the Children's Online Privacy Protection Act (COPPA)[3] and has consistently called for strong regulations to protect children from the risks of connected products.[4] EPIC has explained the risks of the Internet of Things (IoT)[5] and children's toys to the U.S. Congress, the Federal Trade Commission, and the Consumer

[1] Evaluation of the Toy Safety Directive, European Commission, https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-3667279_en.
[2] *About EPIC*, EPIC, https://epic.org/epic/about.html.
[3] *Children's Online Privacy Protection Act (COPPA),* EPIC, https://epic.org/privacy/kids/. *See also EPIC Testimony and Statement to the House of Representatives Committee on the Judiciary*, Sept. 12, 1996, https://www.epic.org/privacy/kids/EPIC_Testimony.html; *EPIC Letter to FTC Commissioner Christine Varney on the Direct Marketing Use of Children's Data*, Dec. 14, 1995, https://www.epic.org/privacy/internet/ftc/ftc_letter.html.
[4] *Children's Online Privacy Protection Act (COPPA),* EPIC, https://epic.org/privacy/kids/.
[5] *See, e.g.*, Internet of Things (IoT), EPIC, https://epic.org/privacy/internet/iot/. *See also, e.g.,* EPIC Letter to the House Committee on Energy and Commerce on Internet of Things Legislation, May 21, 2018, https://epic.org/testimony/congress/EPIC-HEC-IoTLeg-May2018.pdf; Comments of EPIC to the Consumer Product Safety Commission on The Internet of Things and Consumer Products Hazards, May 16, 2018, https://epic.org/apa/comments/EPIC_CPSC_IoT_May2018.pdf; EPIC Warns Congress of Risks of "Internet of Things," EPIC, https://epic.org/2018/01/epic-warns-congress-of-risks-o-1.html.

Product Safety Commission in testimony,[6] agency comments,[7] petitions,[8] and investigative complaints.[9]

I. Internet-connected toys create substantial health and safety risks to children

Privacy and security are critical to ensuring consumer safety. The growth of the Internet of Things (IoT) poses hazards extending far beyond traditional consumer product safety risks. IoT devices control thermostats, home lights and locks, baby monitors, home security systems, and even vehicles. Many IoT devices surreptitiously record private conversations in homes.[10] Poorly secured IoT devices expose consumers to malware, ransomware, and criminal hacking that result in physical harm and harm to property.[11] Last year EPIC joined other consumer advocacy groups in a letter to the CPSC to urge the agency to recall Google Home Mini.[12] Due to a product defect, the Google device was always listening to conversations even when in the "off" position. Users could not disable it. Therefore, both the intentional designs (e.g., Amazon Alexa) and unintentional flaws (e.g., Google Home Mini) of IoT devices present risks to consumers.

Children's toys and wearables[13] are among the most vulnerable types of IoT devices. Recently EPIC, the European Consumer Organization (BEUC), and the Norwegian Consumer

---

[6] Testimony of EPIC to the U.S. Senate on New Technologies and the Children's Online Privacy Protection Act (COPPA), Apr. 29, 2010, https://www.epic.org/privacy/kids/EPIC_COPPA_Testimony_042910.pdf.

[7] *See, e.g.,* Comments of EPIC to the FTC on COPPA Information Collection Requirements, Dec. 3, 2018, https://epic.org/apa/comments/EPIC-FTC-COPPA-Dec2018.pdf; Comments of EPIC to the FTC, "Children's Online Privacy Protection Rule: Entertainment Software Rating Board's Safe Harbor Program Application to Modify Program Requirements," May 9, 2018, https://epic.org/privacy/kids/EPIC-COPPA-ESRB-Safe-Harbor-Comment-05-09-18.pdf.

[8] *See e.g.*, *Consumer and Privacy Groups Demand Action on Toys that Spy on Children*, Dec. 18, 2017, http://www.commercialfreechildhood.org/consumer-and-privacy-groups-demand-action-toys-spy-children; Letter to FTC Chairwoman Maureen Ohlhausen to Investigate Children's Smartwatches, Oct. 18, 2017, http://www.commercialfreechildhood.org/sites/default/files/Smart%20Watch%20FTC%20letter%2010.18%20FINAL.pdf; Petition Against Mattel's Aristotle, Oct. 2, 2017, http://www.commercialfreechildhood.org/sites/default/files/Letter%20to%20Mattel.pdf.

[9] *In the Matter of Universal Tennis*, FTC, May 17, 2017, https://epic.org/algorithmic-transparency/EPIC-FTC-UTR-Complaint.pdf; *In the Matter of In re Genesis Toys*, FTC, Dec. 6, 2016, https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf; *In the Matter of Amazon.com, Inc*., FTC, Apr. 22, 2013, https://www.epic.org/privacy/kids/EPIC_COPPA_Testimony_042910.pdf.

[10] EPIC Letter to DOJ Attorney General Loretta Lynch, FTC Chairwoman Edith Ramirez on "Always On" Devices (Jul. 10, 2015), https://epic.org/privacy/internet/ftc/EPIC-Letter-FTC-AG-Always-On.pdf.

[11] *See, e.g.*, Thomas Brewster, *A Basic Z-Wave Hack Exposes 100 Million Smart Home Devices*, Forbes (May 24, 2018), https://www.forbes.com/sites/thomasbrewster/2018/05/24/z-wave-hack-threatens-to-expose-100-million-smart-homes/#65b4f62e4517; *Security Flaw Could Have Let Hackers Turn On Smart Ovens*, Phys.org (Oct. 26, 2017), https://phys.org/news/2017-10-flaw-hackers-smart-ovens.html; Karl Brauer & Akshay Anand, *Braking the Connected Car: The Future of Vehicle Vulnerabilities*, RSA Conference 2016, https://www.rsaconference.com/writable/presentations/file_upload/ht-t11-hacking- the-connected-car- thetfuturetof-vehicle-vulnerabilities.pdf ; FireEye, *Connected Cars: The Open Road for Hackers* (2016), https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/connected-cars-the-open- road-for- hackers.pdf.

[12] Coalition Letter to U.S. Consumer Product Safety Comm. On Google Home Mini (Oct. 13, 2017), https://epic.org/privacy/consumer/Letter-to-CPSC-re-Google-Mini-Oct-2017.pdf.

[13] Children's Privacy At Risk From Smartwatches, Privacy International, https://privacyinternational.org/examples-abuse/1904/childrens-privacy-risk-smart-watches; *see also* EPIC Letter to FTC Chairwoman Maureen Ohlhausen on the Risks of Children's Smartwatches, Oct. 18, 2017, http://www.commercialfreechildhood.org/sites/default/files/Smart%20Watch%20FTC%20letter%2010.18%20FINAL.pdf.

Counsel called for U.S. and EU enforcement action against companies that sell connected toys that violate consumer privacy laws by exposing young children to continuous surveillance.[14] Germany recently banned Genesis Toys' connected doll, My Friend Cayla, because of the hacking risks from the doll's insecure Bluetooth device.[15] The doll's Bluetooth connection could be compromised to track a child's location, communicate with children, and secretly record their conversations.[16] The Norwegian Consumer Council pointed out these same vulnerabilities in children's smartwatches.[17]

Despite these serious hazards, the Commission does not currently regulate connected toys under the Toy Directive. While "electric toys" are included in the Directive to address safety risks, connected toys are not. In fact, the Commission specifically excludes "electronic equipment" and "interactive software" from the Directive.[18] However, there is no reason to exclude connected toys from regulation. Just as a toy with lead paint poses a safety risk to children, a connected toy also poses a safety risk to children. The current, draft Directive requires developers and manufacturers to implement hygienic designs so that toys can be cleaned to "avoid infection, sickness, or contamination,"[19] but it does not require connected toys to be securely-designed to protect against surveillance and physical risk.

Connected toys should be regulated just like similar non-connected toys. Adding an embedded computer chip to a toy does not diminish the need for safety standards; it increases it.

II. The European Commission should establish official guidelines for the development and distribution of connected toys.

The market for connected toys is rapidly growing, amplifying the need to update the Directive to regulate connected toys. At least 224 million smart toys were shipped worldwide last year,[20] showing how many of the world's top toymakers are "going digital." Many of Mattel's most popular toys[21] already implement AI and Bluetooth technology as part of the company's mission to

---

[14] EPIC, *In re Genesis Toys and Nuance Communications* (December 6, 2016), Complaint on COPPA Violations in "Toys that Spy," https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf; Thomas Claburn, Playtime's Over: Internet-Connected Kids Toys "Fail Miserably" at Privacy, The Register (Dec. 8, 2016), https://www.theregister.co.uk/2016/12/08/connected_toys_fail_miserably_at_privacy/; *Connected Toys Violate European Consumer Law*, Norwegian Consumer Counsel (Dec. 6, 2016), https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws.

[15] *German Parents Told to Destroy Cayla Dolls Over Hacking Fears*, BBC (Feb. 17, 2017), https://www.bbc.com/news/world-europe-39002142; *see also In the Matter of In re Genesis Toys*, FTC, Dec. 6, 2016, https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf.

[16] *In re Genesis Toys and Nuance Communications* (December 6, 2016), Complaint on COPPA Violations in "Toys that Spy," https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf.

[17] Children's Privacy At Risk From Smartwatches, *Privacy International,* https://privacyinternational.org/examples-abuse/1904/childrens-privacy-risk-smart-watches.

[18] Directive, 29-30.

[19] Directive, 45.

[20] Dominic Utton, *Are Toys Out of Fashion? How the Digital Revolution is Killing Off Traditional Playthings*, Express (Mar. 8, 2018), https://www.express.co.uk/life-style/life/928816/toys-r-us-lego-barbie-mattel-digital-revolution-toy-crisis.

[21] *See, e.g., Hell No Barbie: 8 Reasons to Leave Hello Barbie on the Shelf*, Campaign for a Commercial-Free Childhood, https://www.commercialfreechildhood.org/action/hell-no-barbie-8-reasons-leave-hello-barbie-shelf; Sandy Mazza, *Mattel dives into digital toys with new Silicon Valley partnership*, Mercury News (Oct. 2, 2017), https://www.mercurynews.com/2017/10/02/mattel-dives-into-digital-toys-with-new-silicon-valley-partnership/.

"[build] its Power Brands (e.g. FisherPrice, Barbie) into 360-degree connected systems."[22] According to LEGO marketing officer, Julia Goldin, "in the past few years the growth [of connected toys] has been supernatural."[23] Indeed, smart toys are projected to command an $18 billion hardware and software market share by 2023, up from approximately $6 billion this year.[24]

It cannot be overstated that connectivity introduces certain dangers, and that manufacturers, not consumers, must bear the responsibility to ensure the safety and security of their products.[25] The same rationales for regulating the manufacturing and design hazards of consumer products apply to regulating privacy and security hazards, which can lead to physical safety threats.[26] Consumers do not have enough information to evaluate products based on safety or security and companies have little incentive to maintain strong standards without regulation. Regulation of connected toys is critical to ensuring consumer safety and security.

The Commission should revise the Directive to establish mandatory safety regulations for connected toys and require manufacturers to certify compliance with these standards before toys are released to the marketplace. The UK government established a helpful 13-rule framework for manufacturers of IoT products that can be useful to regulate connected toys.[27]

1. No default passwords
2. Implement a vulnerability disclosure policy
3. Keep software updated
4. Securely store credentials and security-sensitive data
5. Communicate securely
6. Minimize exposed attack surfaces
7. Ensure software integrity
8. Ensure that personal data is protected
9. Make systems resilient to outages
10. Monitor system telemetry data
11. Make it easy for consumers to delete personal data
12. Make installation and maintenance of devices easy
13. Validate input data

---

[22] *Mattel Unveils Plan to Reinvent Company and Deliver Enhanced and Sustainable Growth,* Mattel (Jun. 14, 2017), https://news.mattel.com/news/mattel-unveils-plan-to-reinvent-company-and-deliver-enhanced-and-sustainable-growth.
[23] Utton.
[24] *Smart Toys Tipped for Massive Growth*, InsideRetail Asia (May 9, 2018), https://insideretail.asia/2018/05/09/smart-toys-market-tipped-for-massive-growth/.
[25] *See* Alan Butler, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices*?, 50 U. Mich. J. L. Reform 913 (2017), http://repository.law.umich.edu/cgi/viewcontent.cgi?article=1193&context=mjlr; *See also* Bruce Schneier, *Click Here to Kill Everybody* (2018).
[26] Poorly secured mobile applications including KidGuard have enabled stalking and harassment. Jennifer Valentino-DeVries, *Hundreds of Apps Can Empower Stalkers to Track Their Victims*, NY Times (May 19, 2018), https://www.nytimes.com/2018/05/19/technology/phone-apps-stalking.html.
[27] UK Department for Digital, Culture, Media & Sport, *Secure by Design: Improving the cyber security of consumer Internet of Things Report* (March 2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf.

The European Commission should build on this framework to address the risks of connected toys in the Directive and shift responsibility for safety and security back to manufacturers.

Conclusion

Connected toys expose children to greater harms than the non-connected toys covered under the Directive. The European Commission should revise the EU Toy Directive to regulate connected toys and establish mandatory safety standards to address the unique safety and security hazards they pose.

There should be "smart" regulations for "smart" toys.

Respectfully submitted,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Eleni Kyriakides
Eleni Kyriakides
EPIC International Counsel

/s/ Spencer K. Beall
Spencer K. Beall
EPIC Administrative Law Fellow