For immediate release

Contact:
Josh Golin, CCFC (josh@commercialfreechildhood.org; 617-896-9369)
Jeff Chester, CDD (jeff@democraticmedia.org; 202-494-7100)

"Smartwatches" For Parents to Monitor Young Children Actually Pose a Danger to Kids' Welfare

Groups say the products have major security and privacy flaws, call on FTC to act. Strangers can easily seize control of the watches and use them to track and eavesdrop on children.

WASHINGTON, DC – October 18, 2017—A number of brands of "smartwatches" intended to help parents monitor and protect young children have major security and privacy flaws which could endanger the children wearing them. A coalition of leading U.S. child advocacy, consumer, and privacy groups sent a letter to the Federal Trade Commission (FTC) today, asking the agency to investigate the threat these watches pose to children.

Smartwatches for children essentially work as a wearable smartphone. Parents can communicate with their child through the mobile phone function and track the child's location via an app. Some product listings recommend them for children as young as three years old. Groups sending the letter to the FTC are the Electronic Privacy Information Center (EPIC), the Center for Digital Democracy (CDD), the Campaign for a Commercial-Free Childhood (CCFC), the Consumer Federation of America, Consumers Union, Public Citizen, and U.S. PIRG. The advocacy groups are working with the Norwegian Consumer Council (NCC), which conducted research showing that watches sold in the U.S. under the brands Caref and SeTracker have significant security flaws, unreliable safety features, and policies which lack consumer privacy protections. In the EU, groups are filing complaints in Belgium, Denmark, the Netherlands, Sweden, Germany, the UK, and with other European regulators.

"By preying upon parents' desire to keep children safe and, these smart watches are actually putting kids in danger," said CCFC's Executive Director Josh Golin. "Once again, we see Internet of Things products for kids being rushed to market with no regard for how they will protect children's sensitive information. Parents should avoid these watches and all internet-connected devices designed for kids."

The NCC's research showed that with two of the watches, a stranger can take control of the watch with a few simple steps, allowing them to eavesdrop on conversations the child is having with others, track and communicate with the child, and access stored data about the child's location. The data is transmitted and stored without encryption. The watches are also unreliable: a geo-fencing feature meant to notify parents when a child leaves a specified area, as well as an "SOS" function alerting parents when a child is in distress, simply do not work. The manufacturers' data practices also put children at risk. Some devices have no privacy policies at all, and the policies that do exist lack basic consumer protections,

including seeking consent for data collection, notifying users of changes in terms, and allowing users to delete stored data.

"The Trump Administration and the Congress must bring America's consumer product safety rules into the 21st century," said Jeff Chester of the Center for Digital Democracy. "In the rush to make money off of kids' connected digital devices, manufacturers and retailers are failing to ensure these products are truly safe. In today's connected world that means protecting the privacy and security of the consumer—especially of children. Both the FTC and the Consumer Product Safety Commission must be given the power to regulate the rapidly growing Internet of Things marketplace."

The Caref (branded Gator in Europe) and SeTracker smartwatches are available online through Amazon. The groups have asked the FTC to act quickly to investigate these products, and they advise parents to refrain from buying the products because of the danger they could pose to children. The NCC, which conducted the testing of the watches, advises consumers who have already purchased the watches to stop using them and uninstall the app.

"The Federal Trade Commission must be proactive in protecting consumers—especially vulnerable young children—from harmful products that abuse technology for the sake of profit," said Kristen Strader, Campaign Coordinator for Public Citizen. "Smartwatches and similar devices must be absolutely safe and secure before they are released to the public for sale."

Ed Mierzwinski, Consumer Program Director at U.S. PIRG, said, "Companies making any internet-connected devices, but especially for children, need to ensure that privacy and security are more than breakable — or worse, hackable — promises."

Katie McInnis, technology policy counsel for Consumers Union, said, "When a company sells a smartwatch aimed at children, it must ensure the product is safe and secure. The FTC should launch an investigation into the privacy and security concerns surrounding these products to make sure families are safe."

The same trans-Atlantic coalition persuaded government authorities and retailers last December that the internet-connected dolls Cayla and i-Que Robot were spying on children and threatening their welfare, and retailers removed the toys from store shelves. The FBI subsequently issued a warning to consumers that internet-connected toys could put the privacy and safety of children at risk.

###

Short video from the NCC highlighting dangers of smartwatches

Video explaining security flaws in detail