Privacy groups warn of perils in smartwatches for kids

WASHINGTON, US: Smartwatches designed to help parents keep tabs on children could create privacy and security risks, activist and consumer groups said this week as they called for probes by regulators. ***[See update below]***

A coalition of child protection, consumer, and privacy groups asked the US Federal Trade Commission to investigate the risks posed to children by the devices and also called on retailers to stop selling the watches.

The groups said consumer organisations in Europe were expected to file similar complaints with EU regulators.

The organisations contend that the devices, instead of keeping children safe, could make them vulnerable to hackers or criminals.

"Preying upon parents' desire to keep children safe"

"By preying upon parents' desire to keep children safe... these smartwatches are actually putting kids in danger," said Josh Golin of the Campaign for a Commercial-Free Childhood in a statement.

"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 actions come after research by the Norwegian Consumer Council highlighted security flaws in smartwatches designed for children, which transmit and store data without encryption.

With two of the watches, an attacker was able to take control of the watch, eavesdrop on conversations, communicate with the child, and access stored data about the child's location.

The Norwegian group also found that a "geofencing" feature meant to notify parents when a child leaves a specified area did not work as advertised, according to the organisations.

Serious Wi-Fi flaw found in WPA2 protocol

Ilse van den Berg 18 Oct 2017

The study examined smartwatches sold under the Caref brand, marketed as Gator in Europe, SeTracker, Xplora, and Tinitell.

"The devices implicate not only the data privacy of children, but also their personal safety," said a letter to the FTC by the Electronic Privacy Information Center, Center for Digital Democracy, Campaign for a Commercial-Free Childhood, Consumer Federation of America, Consumers Union, Public Citizen and the US Public Interest Research Group.

"The devices create a new vulnerability that allows a third party to find a young child at precisely the time when the child is separated from a parent or guardian."

The same coalition warned last year of similar risks from internet-connected dolls, prompting an FBI warning and leading to many retailers taking the products off their shelves.

Source: AFP

UPDATE

In response to this article, Alcatel sent Bizcommunity the below statement:

> ***Alcatel / TCL smartwatches meet high international information security standards****In response to a recent report that detailed privacy and security flaws across a selection of popular smartwatches for kids, Alcatel / TCL outlines the security features in its smartwatches, which include the Alcatel MoveTime Track & Talk Kids Watch as well as the soon-to-be-launched TCL MoveTime Family Watch.Alcatel / TCL products were not among those evaluated in the report by a security firm hired by the Norwegian Council, however, an image of its smartwatch was used in the article. In light of this, the company would like to take this opportunity to reassure the market that its existing and upcoming smartwatches are built to the latest security standards and technologies to protect the data and privacy of all users, most importantly children.In response to specific concerns raised in the article:*
>
> ## *Affected watches do not have sufficient protection to stop computer hackers*
>
> *Alcatel / TCL follows international industry and national government standards that layout rigorous requirements for information security in the design of TCL products. All data stored on the watch and transported across the network is encrypted—meaning that no one can decode and use it if they are not the authorised user.*
>
> ## *Some manufacturers are violating EU data protection laws*
>
> *Alcatel / TCL manages data in the secure Amazon cloud, retains it for no more than six months, and does not sell personally identifiable information to third parties. Alcatel / TCL uses non-personally identifiable data to improve its products, service, content user experience and performance. Parents have full control over their child's data—if they unpair any Alcatel / TCL watch from the app, all data will automatically be removed from both the device and the cloud.Before we launch any of our products, we do comprehensive security risk assessments, including identity authentication, confidentiality, key security, and service authentication in order to obtain EU/EC authorisation," says Ernst Wittmann,*

global account director MEA & country manager – Southern Africa, at Alcatel. "We believe that the device and its app offers robust security that prevents any unauthorised person from hacking into an Alcatel / TCL smartwatch and accessing data or tampering with features such as geo-fencing and location tracking."

In light of this, Bizcommunity sincerely apologises to Alcatel for using the image referred to in the statement. We specifically tried to source an image with an unbranded smartwatch. However, we have since replaced the image to rectify this.