BEUC The European Consumer Organisation

The Consumer Voice in Europe

ANEC

Raising standards for consumers

Ms Tiina Astola
Director-General
Mr Francisco Fonseca Morillo
Deputy Director General
European Commission
Rue Montoyer 59

B – 1040 Brussels

Ref.: BEUC-X-2017-103
ANEC-SG-2017-G-007

18 October 2017

Subject: Serious security and data protection flaws in smartwatches for children

Dear Ms Astola, Dear Mr Fonseca Morillo,

We write on behalf of BEUC, the European Consumer Organisation, and ANEC, the European consumer voice in standardisation, in order to draw your attention to a study by our Norwegian member, Forbrukerrådet (Norwegian Consumer Council - NCC). The NCC examined smartwatches for children available on the European market and discovered fundamental flaws related to security, privacy, and broader consumer protection.

The Norwegian research confirms and heightens concern about connected products - toys in particular - that we brought to your attention in a similar case in December last year[1]. However, the findings of the study on smartwatches for children are even more alarming and require immediate action, not only by national authorities individually and through their European networks, but also by EU decision makers.

Study on smartwatches for children

The Norwegian Consumer Council carefully examined the terms of use and privacy policies of four smartwatches for children: Gator 2, Tinitell, Viksfjord and Xplora.

Technical tests were also carried out to evaluate the levels of privacy and security protection provided by the watches.

These smartwatches for children are wearable mobile phones that allow parents to use an app on their smartphones to keep in touch with and track the location of their children. Smartwatches available on the European market are often poor-quality products imported (e.g. from China), and rebranded by a vast number of local retailers. This results in a highly chaotic market, with the same watches being available under different names in different countries. This makes it very difficult to identify the watches concerned, or those responsible for their failings.

[1] Our letter of December: BEUC-L-2016-434 / ANEC-ML-2016-0163.

Bureau Européen des Unions de Consommateurs AISBL | **Der Europäische Verbraucherverband**
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.beuc.eu • www.twitter.com/beuc
TVA: BE 0422 071 051 • EC register for interest representatives: identification number 9505781573-45

ANEC, the European Association for the Co-ordination of Consumer Representation in Standardisation
Av. de Tervueren 32, box 27 – 1040 Brussels - +32 (0)2 743 24 70 - www.anec.eu
EC register for interest representatives: identification number 507800799-30

Critical security flaws

Mnemonic, the IT security company which did the technical testing of the watches, discovered **significant security flaws** in three out of the four tested devices. It discovered, for instance, that two devices had flaws that could allow a potential attacker to take control of the apps, thus gaining access to children's real-time and historical location, and personal details, as well as even enabling them to contact the children directly, all without the parents' knowledge.

One of the watches also functions as a listening device, allowing the parent or a stranger with some technical knowledge to monitor the surroundings of the child without any clear indication on the watch that this is taking place.

Two of the watches are in addition vulnerable to the so-called location-spoofing, which means that they can allow the attacker to manipulate the location data sent from the watch to the app on the parent's phone. Hence the attacker could make the watch appear to be in a location other than its actual location.

Needless to say, these security flaws have serious implications for the privacy, and – potentially - for the safety and well-being of the users. Taking into account that the target users of this type of watch are young children, this is particularly alarming.

Conducting an 'attack' on these watches usually requires only a basic to moderate understanding of web communications, and there is no possibility for consumers to protect themselves from the risks brought by these unsafe devices.

Security functions of the smartwatches are not reliable

Smartwatches for children are usually being advertised as a means for parents to feel secure about the location of their children and their wellbeing. Those promises are not being kept. Not only are the devices vulnerable to attacks, as described above, but even the advertised features that are supposed to raise the security levels of children - such as an SOS button that alerts the parents if the child is in distress, and a geofencing function that sends an alert whenever the child enters or leaves a designated area - are unreliable. In practice, this means that the device might in fact provide a false sense of security to parents.

Users' personal data not protected

The analysis of the terms of use and privacy policies revealed that unclear, illegal or sometimes even inexistent, user terms lack compliance with EU data protection legislation.

Only one of the services asks for consent to data collection. Moreover, some of the watches have no functionality to delete user accounts or account history. If the child stops using a watch, further data generation and exposure will be prevented, but an attacker will not be stopped from accessing historical data already recorded.

Finally, several of the devices send data back to obscure servers around the world, with little indication as to how that information is stored, secured or used. Also, children's location data transmitted by one of the services (Gator) is unencrypted.

The watches collect, transmit and store large volumes of information about the user's movements - children in this case. It should be obvious that this data needs to be secure and treated with special care, fully respecting the users' privacy and in full compliance with data protection rules. Unfortunately, this is not the case.

Illegal user terms

Additional flaws in the terms of use of the four smartwatches analysed by the NCC include, for instance, the fact that none of them promises to notify its users about the changes in these terms. At least one companion app (Xplora) allows children's personal data to be used for marketing purposes, while the other three are unclear about how such information may or may not be used.

What needs to be done

In our opinion, the smartwatches for children tested by the NCC **do not respect several EU laws including legislation on personal data protection, radio equipment and horizontal consumer protection legislation.**

As these products are for use by young children, the findings of the NCC research become even more serious. **The products pose a direct safety threat to these users.**

Please note that, ahead of publication of this report, the NCC alerted the Norwegian Data Protection Authority, which in turn notified the importers and manufacturers in question to allow them to rectify the issues. Nevertheless, it seems the watches continue to be actively promoted after the companies were warned of the findings.

- We believe these watches must be remedied immediately or be withdrawn from the market in a coordinated manner at European level. Hence, we urge you to ask national authorities and relevant European networks to take the necessary action.

- Regarding the serious security flaws, we call on the European Commission to take measures to ensure that *mandatory* requirements for technical safeguards are introduced according to the principles of security by default and by design. Consumers should not be at risk when using default settings, and their reasonable expectations to security and safety must be met.

Please note we have also alerted DG Connect and DG Grow about the NCC report.

Please find the link to the complete report of the Norwegian Consumer Council. Our individual press releases can be found on our websites[2].

Please do not hesitate to contact us should you require further information.

Yours sincerely,

Monique Goyens
Director General

Stephen Russell
Secretary General

[2] http://www.beuc.eu/publications/new-research-reveals-alarming-security-flaws-smartwatches-children/html and http://www.anec.eu/images/Publications/press-releases/ANEC-PR-2017-PRL-008.pdf