

Mr Gerd Billen, State secretary,
ICPEN Presidency
Federal Ministry of Justice and
Consumer Protection
(Division for Enforcement of Consumer
Law; Coordination and Cooperation in
the Enforcement of Consumer
Protection)
Mohrenstraße 37

DE - 10117 Berlin,

Ref.: BEUC-X-2016-134/MGO/rs

6 December 2016

Subject: Connected toys do not meet consumer protection standards

Dear Mr Billen,

I am writing to you on behalf of BEUC, the European Consumer Organisation in your capacity as holder of the ICPEN presidency.

Following to our participation to the ICPEN Autumn Conference in Bad Wiessee on the topic of coordinated enforcement, we would like to draw your attention to multiple privacy, security and consumer protection issues discovered recently in relation to a research about 'internet-connected toys', which are currently available to consumers. These issues came to light within the framework of a project carried out by our member Forbrukerrådet (the Norwegian Consumer Council - NCC).

The Norwegian Consumer Council carefully examined the terms of use and privacy policies of three toys: the interactive dolls 'Hello Barbie' and 'My Friend Cayla'; and the 'i-Que Intelligent Robot'. It also commissioned technical tests of the actual functionalities of the toys and their companion apps.

The toys in question connect to the internet and use their build-in microphones and speech recognition technologies in order to engage in 'conversations' with children. The content of children's interactions with the toys may contain sensitive information that the child shared with them in confidentiality.

Through their research, the Norwegian Consumer Council reveals **serious security flaws** as two of the toys (namely My Friend Cayla and i-Que Robot) have no embodied security measures that could prevent unauthorized access to the toy's microphone and speakers. This means that anyone with a Bluetooth functionality on his phone can connect to a toy and use it as a listening device or communicate through it with the child if this person stays within the 15-meter radius (or less if he tries to connect through the wall) while the toy is switched on and not already paired with another device. Needless to say that if someone with bad intentions takes advantage of this security flaw **children and their privacy can be put at serious risk**.

.../...

.../...

If the manufacturer chooses to use cheaper or simplified components in this type of devices, which might be the reason behind the discovered flaws, this could lead to serious security vulnerabilities and could allow for targeted attacks that could compromise children's safety. This aspect should be addressed as soon as possible by the authorities across the world.

Moreover, the analysis and testing carried out revealed that the **toys do not meet the data protection standards**. For example:

- The companies behind those toys reserve the rights to share children's personal data with unspecified third parties;
- The companies fail to properly identify or restrict the purposes for which they use and distribute children's voice data;
- The companies may use children's data for analytical and research purposes unrelated to toys themselves;
- Toys may collect children's data for advertising purposes and separate or explicit consent for the use of data for this purpose is not asked;
- No clear data retention procedures are put in place and in some cases companies request access to data which does not seem necessary for the functioning of the toys;
- Companies transfer children's voice data to third parties, who may use this data for a vast array of purposes;
- In case of the Hello Barbie doll, parents may listen to and share children's private conversations via their apps dashboard.

In relation to the specific contract terms and the conditions of purchase the following issues were identified:

- Their terms and conditions are often not easily accessible and not simple to understand for a regular consumer;
- The companies are not committed to notify users when changing their terms and conditions;
- The service providers reserve their right to terminate the services at any time without notice;
- The companies require from consumers to read not only their own terms and conditions but also those of third party service providers;
- The toys are embedded with pre-programmed phrases endorsing specific commercial products, which constitute a product placement directed to children playing with the toy.

In our opinion, the companies that manufacture these **toys are not respecting consumers' protection standards**. The fact that these products are specifically used by children makes these companies practices even more aggravating.

We consider that these problems merit to be addressed in a coordinated manner at the international level. Therefore, we would kindly request to have the possibility to present the results of the study at a next meeting of the International Consumer Protection and Enforcement Network (ICPEN network).

.../...

.../...

Please note that we have notified also the European Commission and asked them to inform the corresponding networks on the European level (Consumer Protection Cooperation (CPC) Network, Product Safety Committee). We have also written to the chair of the Art 29 Personal Data protection committee. Many of our member organisations will also inform their authorities directly.

BEUC's press release on this topic can be found on our website¹ and the full report with the findings of the analysis carried out by Forbrukerrådet, published today, is available at their website². We also attach the complaints that NCC sent to their national authorities. Please do not hesitate to get back to us should you require any further information.

Yours sincerely,

Monique Goyens
Director General

Enc.: 2

¹ www.beuc.eu

² For more information see: <http://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws>