FORBRUKERRÅDET

The Norwegian Directorate for Civil Protection
postmottak@dsb.no

Oslo 6.12.2016

Letter of concern regarding user agreements and privacy policies for internet-connected toys – the Cayla doll and i-Que robot

We are writing to express our concern about two toys capable of connecting to the internet via an app. The toys in question are the Cayla doll and the i-Que robot, both of which are being sold in Norway.

The Consumer Council has examined the terms for downloading and using the apps, and has commissioned a technical test of the toys. The technical tests carried out by the technology consultants Bouvet, found that the doll and robot offer inadequate user security.

See the attached report "*Analysis of consumer and privacy issues in three internet-connected toys*" (appendix 1) and the technical report "*Investigation of privacy and security issues with smart toys"* (appendix 2), which provide details of our findings.

We have attached a copy of our complaint letter to the Data Protection Authority and the Consumer Ombudsman for your information (appendix 3).

The Consumer Council has asked the regulators to study the attached documentation, and to establish whether the regulations on product safety can be applied.

Background
An increasing number of objects can be connected to the internet. This offers many new opportunities, while at the same time reinforcing and creating new challenges for consumers.

In 2016, the Consumer Council conducted a project looking at the challenges consumers face in relation to the internet of things. We have studied user agreements and privacy policies in selected product categories, and we have carried out technical tests of the products. One part of this project involved investigating connected toys. There is not yet a wide range of internet-connected toys available on the Norwegian market, but this is likely to be a developing and expanding market. The Consumer Council see children as a vulnerable group of consumers, and believe that they are entitled to particular protection.

The Norwegian Consumer Council
Postboks 463 Sentrum, 0105 Oslo, Business registration no. 871 033 382
Telephone (+47) 23 400 500, post@forbrukerradet.no

The products Cayla and i-Que

The toys are manufactured by Genesis Toys, but there is no company information on its website, www.genesis-toys.com. However, the website does link to a privacy policy for Genesis, which provides an address in Hong Kong[1]. There are different European importers of the toys, and there may be multiple importers of the toys to the same country. From what we have been able to establish, the importer of the toys in Norway is Top Toy Norge AS (business registration number 991 492 704). The toys are being sold in Norway by the large toy retail chains Toys R Us and BR-Leker, amongst others.

The number of app downloads could give some indication of the toys' popularity. The Cayla doll appears to be the more popular of the two, and from what we can see, the Norwegian app has been downloaded from Google Play between 10,000 and 50,000 times[2]. The app associated with the i-Que robot is less in demand, with between 1,000 and 5,000 downloads from Google Play[3].
The number of Apple App Store downloads is not available to the public. Yet there is no reason to believe that it is lower than the number of Google Play downloads.

The Cayla doll was named toy of the year in both Norway and Sweden in 2014, according to a sticker on the packaging. The toys are actively marketed in this year's Christmas catalogues from both Toys R Us and BR-Leker. The toys are being sold worldwide.

Cayla and i-Que are interactive toys that can connect to an app on a mobile phone or tablet through a Bluetooth connection. The toys contain a Bluetooth-connected microphone and speaker, while the actual data processing takes place in the app. When the child asks Cayla or i-Que a question, the app translates what the child is saying into text before searching a database for an answer to the question. If the child asks the toy a personal question such as "What is your favourite colour?", the toy obtains the answer from its database without using the internet. If the child asks the toy something that is not in the database, the toy uses the internet services Wikipedia and Weather Underground to find an answer.

The toys contain safety mechanisms / software that automatically check words against a list of blocked words before answering. If the question or answer contains a word from the list of blocked words, the toys will tell the child that they are unable to answer.

Technical findings

The consulting firm Bouvet was asked by the Consumer Council to carry out a technical test of the toys. Bouvet looked at various aspects of the toys' technology – in the actual doll, in the app, and in the data traffic between the two and between the app and the internet. Two aspects of the toys are grounds for particular concern.

[1] Genesis Industries 8/F, HK Spinners Industrial Building, 818 Cheung Shan Wan Road, Kowloon, HK
[2] https://play.google.com/store/apps/details?id=com.toyquest.Cayla.no
[3] https://play.google.com/store/apps/details?id=com.toyquest.iQue.no

1. Basic and insecure connection

When connecting the toy and the mobile/tablet, you must first switch on the toy, and then the mobile/tablet must search for Bluetooth devices. The toys quickly appear on the mobile/tablet under the names Cayla and i-Que, and at the click of a button, the mobile/tablet and the toy have been paired.

You do not need to have physical access to the toy in order to connect to it. As long as the toy is switched on and not connected to another device, any Bluetooth-enabled device is able to search for the toy and connect to it. By using two smartphones, the toys can easily be used to make contact with and communicate with the child. The distance between the toy/child and the devices used to make contact can be relatively long.

The Consumer Council believes that this basic and insecure connection poses a security risk. This security risk could easily have been avoided by implementing security measures when connecting the toys to a device. One such measure could be requiring physical access to the toy before connecting to it. This could involve a physical button on the toy that must be held down while pairing with a new device, or that the user must supply a password when pairing with a new device. Such a password could be affixed to the toy itself, for example. Methods like these are often used on other internet-connected products such as activity wristbands.

2. Security in physical components

Both i-Que and Cayla contain an adapted printed circuit board with a Bluetooth module based on chip IS1685S from ISSC. The Bluetooth module in Cayla supports Bluetooth 2.1 Secure Simple Pairing. The technical report, see page 14, produced by Bouvet highlights the following statement from a group of Bluetooth experts, which explains that *"useful whenever product implementers want to make the user experience easier and have accepted the increased risk of security attacks".*

The Consumer Council therefore deems it likely that the manufacturer has rated user-friendliness higher than the security aspect.

The Consumer Council is particularly alarmed that the issue of poor user security has already been identified in the past. The problem was one of several flaws highlighted by the BBC as early as January 2015, when a security expert easily hacked into Cayla and was able to control what she was saying[4]. The manufacturer responded that they would update the app. Despite this promise, our technical test found that user security has not improved. We would like to remark that since the technical component within the Cayla doll has insufficient security measures, and an update of the app would therefore probably not remedy the flaw.

Potential consequences of poor user security

[4] http://www.bbc.com/news/technology-31059893

By using a single smartphone, anyone can connect to the toys and play sounds through them. For instance, this would allow strangers to play scary or inappropriate sound clips, which could cause stress and distress to the child. By using two phones, one phone can be used to connect to the toy, and the other can be used to call the first phone. This allows the caller to both speak and listen via the toy as if it were an ordinary Bluetooth headset. This means that the toy can be used to eavesdrop on the room that the toy is in, or to communicate with the child.

In a worst case scenario, a stranger can thus talk to the child through the toy. The use of the Bluetooth names “Top Toy Cayla” and “i-Que Robot” also makes it easy to identify insecure devices in an area. It should be pointed out that Cayla is being marketed as “your new best friend”, and the poor user security could therefore be regarded as representing a particularly serious breach of trust.

You can prevent unauthorised access to Cayla by always switching off the doll after use or by permanently having the doll connected to another device. It is likely that the mobile/tablet being used with the toy will often be disconnected by being out of range (e.g. when parents take the phone with them when leaving home), and that children will not think to switch their toys off after use. This means that the vulnerability can be subject to misuse in many situations.

It is particularly worrying that products aimed at children deploy vulnerable communication standards such as Bluetooth without security measures, which do not prevent unauthorised users from connecting.

The Consumer Council’s European umbrella organisation, BEUC, will approach the EU Commission’s Expert Group on Toy Safety, to present the Norwegian Consumer Council’s findings in the two above-mentioned reports.

We urge the Directorate for Civil Protection to investigate whether the product safety regulations can be applied in a case like this, which comes with the added dimension of children being involved.

Best regards
The Norwegian Consumer Council

Randi Flesland
Director
The Norwegian Consumer Council

Finn Myrstad
Technical Director, Digital Services
Finn.myrstad@forbrukerradet.no

Appendix 1: *"Analysis of consumer and privacy issues in three internet-connected toys"*
Appendix 2: *"Investigation of privacy and security issues with smart toys"*
Appendix 3: *Complaint to the Data Protection Authority and the Consumer Ombudsman regarding the terms of use for the toys*

The Norwegian Consumer Council
Postboks 463 Sentrum, 0105 Oslo, Business registration no. 871 033 382
Telephone (+47) 23 400 500, post@forbrukerradet.no