#Toyfail

An analysis of consumer and privacy issues in three internet-connected toys

Desember, 2016

FORBRUKERRÅDET

Content

Summary

The current trend of attaching sensors to a broad variety of devices, and connecting them to the internet, is usually referred to as the internet of things (IoT). This technology has also spread to the world of children's toys, where several products are already being marketed as "interactive" in unprecedented ways. The popular dolls My Friend Cayla and Hello Barbie, and the robot i-Que, respond to children's voices by using microphones and speech-recognition technologies, using an internet connection and companion app to allow children to have "conversations" with their toys.

As a part of a larger project centering on the IoT, the Norwegian Consumer Council (NCC) has looked at the terms and conditions and technical features of these three connected toys. By virtue of being targeted toward children, an especially vulnerable group of consumers, issues related to consumer rights, security, and privacy was highlighted through the NCC's study.

When scrutinizing the terms of use and privacy policies of the connected toys, the NCC found a general disconcerting lack of regard to basic consumer and privacy rights. The companies behind the toys make claim to wide licenses to use and distribute children's voice data, while failing to properly identify or restrict the purposes for which such information may be used. Potential changes to the terms are not communicated to the users, which makes it very difficult to ensure that proper consent is maintained.

Furthermore, the terms are generally vague about data retention, and reserve the right to terminate the service at any time without sufficient reason. Additionally, two of the toys transfer personal information to a commercial third party, who reserves the right to use this information for practically any purpose, unrelated to the functionality of toys themselves. All of these factors are at edge with Norwegian and European legislation, and indicates that these manufacturers and service providers do not take the consumer and privacy rights of their customers (and their children) sufficiently seriously.

In addition to analyzing legal documents, the NCC commissioned a technical report on the actual functionalities of the toys and companion apps. In this technical study, it was discovered that two of the toys have practically no embedded security. This means that anyone may gain access to the microphone and speakers within the toys, without requiring physical access to the products. This is a serious security flaw, which should never have been present in the toys in the first place.

Furthermore, the tests found evidence that voice data is being transferred to a company in the US, who also specialize in collecting biometric data such as voice-fingerprinting. Finally, it was revealed that two of the toys are embedded with pre-programmed phrases endorsing different commercial products, which practically constitutes product-placement within the toys themselves.

These discoveries are another sign that emerging IoT-technologies may not be well suited for children's products. Unless the manufacturers and service-providers are willing to take these issues seriously, the NCC are concerned that the area

of connected toys is rife with potential risks for children's safety and wellbeing, as they play and interact with these products.

The internet of toys

As the IoT becomes widespread, an increasing number of devices and appliances are fitted with sensors and connected to the internet. Everything from toothbrushes and umbrellas to refrigerators and cars are being sold with internet-related functions. This allows the devices to communicate with each other, and to transfer data to third parties for analytical and other purposes. As the technology becomes ubiquitous, a myriad of new opportunities arise. For example, your connected car might tell your smart-home center that you are on your way home from work, causing a connected thermostat to turn up the heat so your home is at a comfortable temperature when you arrive there. Seamless integration between devices such as these may simplify everyday life and make it more comfortable.

On the other hand, the IoT also brings new and familiar issues in its wake. Many companies and manufacturers that have little or no experience with creating digital services are moving into the uncharted IoT territory. This could potentially lead to problems such as little understanding of or concern for digital security and privacy protection. When a wide spectre of devices record and disseminate enormous streams of information, questions arise of who has access to this data, and about how it might be used.

Insufficient security measures are another rising area of concern, exemplified in the case of hacked smart cars, where white hat hackers were able to take control over a Jeep Cherokee while it was speeding down the highway.[1] There have also been cases of devices simply stopping working as intended, either because of shoddy design, or because the online servers necessary for key functions are no longer maintained by the service providers.[2] These are some of the issues that have led the NCC to undertake a project focused on the IoT.

This project, which began with looking at fitness wearables,[3] maps some popular and rising areas of "smart" technologies, and examines whether these properly uphold the outlined areas of privacy, security, and general consumer protection.

One of the areas where internet connections are becoming integrated into traditionally analogue products is in children's toys. The Norwegian Consumer Council has looked at the legal terms and interactive functions of three such products. The three toys that were analysed are the interactive dolls Hello

1 https://www.washingtonpost.com/news/morning-mix/wp/2015/07/22/car-hacking-just-got-real-hackers-disable-suv-on-busy-highway/ [accessed 08-11-2016]

2 https://www.theguardian.com/technology/2016/apr/05/revolv-devices-bricked-google-nest-smart-home [accessed 08-11-2016]

3 http://www.forbrukerradet.no/siste-nytt/fitness-wristbands-violate-european-law [accessed 08-11-2016]

Barbie[4] and My Friend Cayla[5], and the i-Que Intelligent Robot.[6] The latter two were chosen because they are sold in most major toy stores in Norway, and are some of the first "smart" toys to gain popularity. Hello Barbie was added to the study because Barbie is one of the best known dolls in existence, signifying the entry of the big league toymakers into the world of the IoT.

The products

My Friend Cayla

My Friend Cayla, or Cayla for short, is an interactive doll that connects to an app on a mobile phone or tablet, through a Bluetooth connection. The companion app is connected to the internet, allowing the doll to answer questions by submitting queries to the websites Wikipedia and the Weather Underground.

Cayla comes with a number of pre-programmed sentences and responses that simulate a conversation with the user, supplemented by pulling additional information from the aforementioned websites. The doll uses speech recognition technology in order to "understand" what the user is saying, which allows children to ask questions ranging from simple conversational topics ("What is your favorite color?"), to fact-based queries ("What is the capital of Norway?"). This happens on a remote server provided by the speech recognition service provider Nuance Communications.[7]

The doll itself contains a Bluetooth connected microphone and speaker, while the mobile application takes care of the data processing. Before use, Cayla has to be connected to a mobile device and turned on by flipping a switch on the back of the doll.

The doll is produced by the Los Angeles-based company Genesis, and is available in stores in North America and in large parts of Europe. The Norwegian-language version of the app has between 10 and 50 000 downloads in the Play Store[8], and Cayla can be bought in most major toy stores, including BR Leker[9] and Toys R Us.[10] She was also voted "Most innovative toy of the year" by the London Toy Industry Association in 2014,[11] and according to the packaging, won a "toy of the

4 http://hellobarbiefaq.mattel.com/

5 http://www.myfriendcayla.com/

6 http://www.ique-robot.com/

7 http://nuance.com/

8 ITunes number of downloads are not publically available, but come in addition to the Play Store number.

9 https://www.br.no/vaare-kategorier/dukker-dukkehus-og-tilbehoer/interaktiv-dukke/my-friend-cayla-interaktiv-dukke?id=632999&vid=082233 [accessed 18-11-2016]

10 http://www.toysrus.no/serier/my-friend-cayla/my-friend-cayla-interaktiv-dukke?id=632999&vid=082233 [accessed 18-11-2016]

11 http://ttpm.com/p/14825/genesis-toys-/my-friend-cayla/

year"-award in both Sweden and Norway the same year. Although the doll has been on the market for a few years, as of November 2016 it is still being heavily marketed through major Norwegian toy stores and in their 2016 Christmas toy catalogues.[12][13] The doll is priced at around 600,- NOK, or about $70.

i-Que

The i-Que Intelligent Robot is, like Cayla, produced by Genesis, and mostly functions in the same ways as the doll. It connects to an app through Bluetooth, and the app connects to the websites Wikipedia and the Weather Underground to find answers to a large variety of questions. The robot also uses speech recognition technologies provided by Nuance Communications to "understand" questions. Additionally, i-Que comes with pre-programmed phrases, a number of different games (from "10 questions" to tic-tac-toe), and different sound effects and movements. The expanded functionality from Cayla is reflected in a higher retail price, costing around 1050,- NOK, or around $120.[14] Like Cayla, i-Que is also available in most Norwegian toy stores, with the Norwegian app having between 1000 and 5000 downloads in the Play Store.

As a side-note, whereas the Cayla doll is marketed toward young girls, i-Que is clearly targeted at boys. While Cayla is eager to talk about playtime, flowers, and cooking, i-Que tends toward scientific facts and telling silly jokes. According to the packaging, both i-Que and Cayla are meant for kids of age 4 and up. Because both toys are produced by the same company, the accompanying terms and privacy policies are nearly identical. The NCC have chosen to look at both because they are both among the most popular connected toys on the market, and are aimed at different segments of children (boys and girls). Due to the different pricing and functionality, it was also relevant to see how the security measures in the two toys compared.

My Friend Cayla & i-QUE

- Toys that connect to the internet in order to answer questions.
- Connects to a companion app through Bluetooth.
- Produced and distributed by Genesis in the U.S., Scandinavia, South Africa, the Middle East (as described on website), Australia, and the Netherlands.
- Distributed by Vivid in the U.K., France, Germany, Austria, Switzerland, and Ireland.
- Uses speech-to-text technology provided by Nuance Communications.

12 http://ipaper.ipapercms.dk/TopToy/RBU/BR/BRNO/16XB/ pp 64 [accessed 21-11-2016]

13 http://ipaper.ipapercms.dk/TopToy/RBU/TRU/TRUNO/16XT/ pp 58 [accessed 21-11-2016]

14 http://www.br.no/vaare-kategorier/radiostyrte-leker/radiostyrt-robot/i-que?id=607353&vid=062591 [accessed 18-11-2016]

Hello Barbie

The Barbie doll line of products is one of, if not the most successful children's toys of all time. Produced by the American company Mattel, Hello Barbie marked the product line's first foray into the world of connected toys. Released in 2015, Hello Barbie uses voice recognition technologies, supplied by the company ToyTalk, in order to simulate conversations with the user.[15] ToyTalk are a company specializing in connected and voice-activated toys, and have a licensing agreement with Mattel where they supply software to the physical toy and app. Before first-time use, the doll is connected to a companion app using wi-fi technology, and the apvp is connected to ToyTalk's servers. Upon subsequent use, the doll connects directly to the internet. Additionally, parents have to create an account with ToyTalk, where they are given access to a dashboard containing the recorded voice clips.

Unlike Cayla and i-Que, Hello Barbie does not connect to third party websites to find answers to children's questions. Instead, the doll comes exclusively with pre-recorded phrases and conversational tidbits that are supposed to adapt to what children are saying. As will be elaborated upon in the analysis below, ToyTalk also uses the recorded children's voice data in order to improve and research their speech technologies. Although Hello Barbie is currently only available in North America, the NCC has chosen to look at the toy because of Barbie's prominent position amongst children's toys. The popularity of the Barbie brand also leads the NCC to believe that the product may be released on the European market in the future. According to the packaging, Hello Barbie is aimed at children of age six and up. She is priced at between $28 and $100.[16]

Hello Barbie

- Toy that uses speech recognition to hold "conversations" with children.
- Connects to the internet through a wi-fi connection.
- Only talks using pre-recorded phrases.
- Produced by the toy company Mattel.
- Speech recognition technology is supplied by ToyTalk.

15 https://www.toytalk.com/

16 https://www.amazon.com/dp/B012BIBAA2/sr=8-1/qid=1479461432/ref=olp_product_details?_encoding=UTF8&me=&qid=1479461432&sr=8-1 [accessed 18-11-2016]

Methodology

For the analysis of the three toys, the Norwegian Consumer Council was interested in seeing how the companies adhere to consumer rights and privacy protections. These issues are especially important since children are a vulnerable group of consumers, who should be given extra precautionary protection in order to prevent breaches of trust and misuse of sensitive information. Particularly because of the voice-driven capabilities and internet connectivity of the toys, the NCC were also interested in seeing how the devices implemented privacy- and security measures.

The analysis consists of two main parts so as to best assess consumer, security, and privacy issues in the connected toys. In order to evaluate the degree of consumer protection afforded, the NCC carefully examined the terms of use and privacy policies of each. Since the actual data processing happens not in the actual toys, but in the companion apps and in cloud servers, the analysis focused on the terms pertaining to the apps, rather than general terms from the toymakers.

The analysis of the terms was done by formulating a set of criteria for good consumer protection practices. As a base for our analysis we apply the Data Protection Directive[17] and the Directive on Unfair Contract Terms in Consumer Contracts[18]. We applied these criteria by locating and reading the relevant documents and judging whether they adhered to the benchmarks. In some cases this was also done to suggest ways in which the companies can improve, and hence the criteria are also based on the recently adopted General Data Protection Regulation (GDPR).[19]

Subsequently, we marked each of the findings on a colour-graded scale, where green means that the criteria are fulfilled, red means unfulfilled, and yellow means that we could not be sure, usually due to unclear terms. For this evaluation, we chose to take the terms at face value, regardless of the technical findings. This is because the terms are the only way for consumers to inform themselves of the practices of the companies behind their devices, with technical testing being reserved for experts and studies such as this.

In order to evaluate the security and privacy measures taken by the companies behind these toys, the NCC contracted the consultancy firm Bouvet to do a number of technical tests. The technical analysis is detailed in a separate technical report (attached),[20] but some of the main findings are included toward the end of this main report. The NCC were interested in seeing how children's data is actually being protected and used in practice, and whether security

17 Directive 95/46/EC - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

18 Directive 93/13/EEC - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31993L0013:en:HTML

19 Regulation (EU) 2016/679 - http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679

20 *Investigation of privacy and security issues with smart toys* – http://www.forbrukerradet.no/undersokelse/2016/toyfail-consumer-and-privacy-issues-in-connected-toys

measures are in place to prevent unauthorized access. This testing was done using both an Apple and an Android device in order to assess the security and privacy-protective measures taken by the manufacturers.

Toward the end of the report, some general implications of and reflections on the findings will be discussed. This includes some ethical considerations that, while not explicitly within the scope of the report, remain relevant to consider, particularly because children are the intended user group.

Analysis of terms

Accessibility: Are the terms easily available?

Before a consumer has the opportunity to ascertain the terms for a product of service, they have to be able to actually locate and access the relevant documents. According to the Data Protection Directive, a legal ground for processing personal data[21] is consent, and we consider consent the relevant legal ground of any such processing in this context.

Both terms and conditions and privacy policies should be easily available through the app stores, and on the official website of the product and/or company. Additionally, it should be clear whether the documents apply to the actual product/service, to the website itself, or both, and whether there are exceptions (for example if there are overriding terms for parts of the service). Thus the criterion is that the documents must be made easily accessible for the average consumer.

1. Accessibility:
Are the terms easily available?

	 Hello Barbie	 Cayla	 iQue
The terms are easily available online	✓	?*	?*
I get the opportunity to read the terms before accepting them	✓	✓	✓

* *Difficult to find the applicable terms. No terms linked from app stores.*

21 Directive 95/46, article 7

Although Hello Barbie is a product of both Mattel and ToyTalk, Mattel's site for the toy makes it clear that the ToyTalk privacy policy and terms are the relevant ones.[22] These terms are available both through ToyTalk's site, and through the app stores.

Cayla and i-Que's terms are not as easily found, as the company operates with different distributors in different regions. Some terms apply to UK users, through the British distributor Vivid or the Hong Kong-based app-distributor ToyQuest,[23] while the one operated by Genesis apparently do not.[24] Making things more confusing, the latter does not have easily accessed terms of use, while the former does.[25] In Cayla's terms of use (or User Agreement), a link is provided to a privacy policy. However, this link[26] leads nowhere, and just redirects the user back to the Cayla splash page. As far as the NCC have been able to find out, ToyQuest are providers of the app, and Genesis of the toy. However, in both set of terms these two companies' contact information point to the same Hong Kong address.

I-Que's user agreement also links to a privacy policy, but this link simply refers back to the user agreement itself.[27] Additionally, the in-app terms for Cayla link to a nonfunctional .pdf that is supposed to be the privacy policy, and later in the document, to ToyQuest's cookie and privacy policy. Therefore, the NCC have used the latter in this analysis, as it is the only relevant privacy policy that could even be found. As a side note, the actual user agreements mostly deal with restrictions put on the user and the rights of ToyQuest, while the consumer's rights are afforded little space.

Since the ToyQuest-based user agreement references the app specifically, the NCC have chosen to use Genesis' Cayla privacy policy, and ToyQuest's user agreement. The same goes for i-Que, which uses nearly identical terms except for a few words that are different. None of the Cayla or i-Que documents are linked to from Google Play, making them even less intuitive to locate for the average user.

It is also important that the existence of terms are made explicit upon first starting the app, so the user (or parent) is made aware of them before giving their consent. This is necessary in order to make informed consent possible. Here, all of the apps have a pop-up when first opening the apps, letting the users look at the policies before clicking "I agree". In addition to displaying the terms in-app, Hello Barbie also provides a short and concise privacy notice that explains its key privacy-related functions in an understandable way. This makes it easier and far more likely that users (or parents of users) will actually consider privacy-related matters related to the product.

22 http://hellobarbiefaq.mattel.com/ [accessed 27-10-2016]
23 http://myfriendcayla.co.uk/privacy [accessed 27-10-2016]
24 http://www.myfriendcayla.com/privacy-policy [accessed 27-10-2016]
25 http://myfriendcayla.co.uk/agreement [accessed 27-10-2016]
26 http://myfriendcayla.com/myfriendcaylapri.html [accessed 27-10-2016]
27 http://ique-robot.co.uk/user-agreement#_7._Privacy [accessed 27-10-2016]

Readability

Once the terms have been located, the next step is to sit down and read them. This is of course rarely done in practice, as terms are notoriously long and complicated, especially when presented on a small screen such as a smartphone or tablet device. In addition to length, the NCC looked at whether the services have made an effort to make the terms understandable, for example by avoiding overly vague statements and hypothetical language, structuring the text for readability, and so on.

Whereas Hello Barbie clearly aims its legal documents toward a parent or guardian, who has to give consent on behalf of the child through a parent verification and account-system, the terms for Cayla and i-Que open with a rather awkwardly formulated statement:

> *"**BEFORE YOU START TO ENJOY PLAYING WITH YOUR NEW FRIEND CAYLA, PLEASE READ THESE TERMS CAREFULLY** BEFORE DOWNLOADING THE MY FRIEND CAYLA APP […] YOU AGREE TO BE BOUND BY THESE TERMS OF USE OR IF YOU ARE A PARENT OR GUARDIAN YOU AGREE TO YOUR CHILD DOWNLOADING AND USING THE APP IN ACCORDANCE WITH THESE TERMS OF USE."*

Cayla terms of use, emphasis added

Although the terms must be interpreted to be directed at parents, the above quote makes it seem like the document is aimed toward children. Hello Barbie's terms, on the other hand, use a more exact definition of who the consenting parties are:

> *""YOU" MEANS EACH PERSON WHO ACCESSES OR USES THE COMPANION APPS OR THE SERVICES (INCLUDING, BUT NOT LIMITED TO YOUR CHILDREN, AS DEFINED HEREIN), WHETHER OR NOT SUCH PERSON PERSONALLY INSTALLED THE COMPANION APPS OR PERSONALLY UTILIZES THE SERVICES. FURTHER, "YOUR CHILDREN" OR "YOUR CHILD" REFERS TO YOUR CHILD, YOUR CHILDREN, OR A CHILD OR CHILDREN UNDER YOUR GUARDIANSHIP OR SUPERVISION."*

Hello Barbie terms of use

Because terms have to be understood in order to give informed consent, the NCC set a criterion of using clear wording and accessible structure.

2. Readability: Are the terms written in clear language and with a user-friendly layout?

	 Hello Barbie	 Cayla	 iQue
Word count	7600 + FAQ (850)	6250	6250
The service uses clear language	✓	?*	?*
The service have made an effort to make the terms readable (layout, etc)	?**	✗	✗

* *PP is clear, ToS are quite legalistic.*

** *Uses Caps Lock.*

The Hello Barbie terms and privacy policy are 7600 words long, while both i-Que and Cayla contain 6250 words each. This is the equivalent of about 15-20 pages of terms for each toy. All three sets of terms use a lot of hypothetical language (e.g. using "we may"), which tells the reader little about what the service will actually do:

> *"We may store and process personal information in the United States and other countries."*
>
> Hello Barbie privacy policy

Additionally, all of the documents use a lot of caps lock throughout,[28] and Cayla and i-Que's terms are full of big blocks of text, even containing repeated paragraphs, making the documents very difficult to parse. These factors all contribute to the fact that the terms and privacy policies are quite difficult to read and understand, undermining the concept of informed consent.

28 Although it is common in the US to employ all caps in order to denote that parts of a legal text is 'conspicuous', it is the NCC's opinion that this is a solution that is not sufficiently user-friendly for the consumer.

Notice about changes

If a user has downloaded the apps and affirmed their consent to the terms, it remains important that the services cannot unequivocally make major changes to the documents. If the services make any material changes to the documents (meaning changes to user rights, functionality, etc.), the users should be notified in advance, so that they have the option to withdraw their consent before being bound by the new terms. As a criterion, this should be communicated clearly, either in the app itself, or through an e-mail notification if the user's e-mail has been supplied.

3. Advance notice: Will the service notify me in advance if they change their terms?

	 Hello Barbie	 Cayla	 iQue
I will be given advance notice if terms are changed	?*	✕	✕

**Will notify in advance about changes to the ToS, but not the PP.*

4. Notice: Will the service notify me by appropriate means?

	 Hello Barbie	 Cayla	 iQue
The service will provide me with appropriate notice if the terms are changed in a way that changes functionality, rights, or user interface.	✕	✕	✕

Hello Barbie's privacy policy does not specify whether they will notify users in advance of changes, while their terms and conditions say that they will operate with a 30 day "notice period". In the privacy policy, it is also stated that users will be given additional notice in the case of material changes. However, the

concept of "additional notice" is very broadly used, including "*such as adding a statement to our web site's homepage or sending you a notification) and/or obtain your prior verifiable consent*" (Hello Barbie privacy policy). This is, in the NCC's opinion, too weak a promise, since adding a statement to a website is not sufficient to properly notify users of material changes.

Both Cayla and i-Que are very noncommittal about giving users any notice about changing their terms, with their privacy policies saying that "*This Privacy Statement may be updated from time to time* **so you may wish to check it each time you submit personal information to us."** (i-Que and Cayla privacy policy, emphasis added). Additionally, both sets of terms and conditions state that

> *"we will do our best to give you advance notice by posting the change on our website (…) You should look at the website regularly to check."*
>
> Cayla and i-Que terms and conditions

In practice, this seems to imply that users are encouraged to read Cayla and i-Que's 15-page legal documents every time they want to play with the toy. Of course, this is an absurd scenario, and since the companion apps are required interfaces, the services should be able to give notification about changes within the app itself. As a side note, changing the terms of children's toys has an additional dimension when considering the practical effects of not accepting the new terms. If parents do not agree with the updated terms, they are put in the awkward position of having to take their children's toy away.

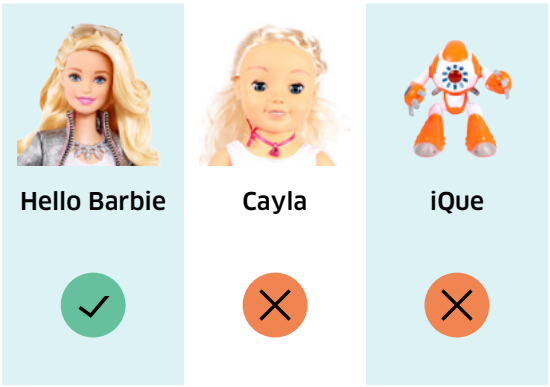
The NCC questions whether the above-mentioned issues in Cayla and i-Que may constitute a breach of the Directive on Unfair Contract terms in Consumer Contracts. This directive is meant to prevent unbalanced relationships of power between the consumer and service provider. Even if individual contractual terms are not deemed to be unfair, the totality of the agreement can still be considered unfair to the user.

Defining personal data

Understanding how a service provider will protect user data relies on how they choose to define "personal data". Under European legislation, personal data is clearly defined and granted special protections related to privacy and security. Since a significant part of the digital environment consists of transfer and processing of personal data, it is essential that the data processors make it clear what they consider personal data.[29] Therefore, the criterion here is that the concept of personal data should be clearly defined and explained in the terms.

29 In the U.S., children's personal information is regulated by the Children's Online Privacy Protection (COPPA) act. (https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule)

5. Definition of personal data: Does the service explain what they categorize as personal data?



None of the three toys analysed by the NCC give a clear explanation of how they classify personal data. This makes it difficult to ascertain how they will protect consumers, for example because it is unclear whether they will consider voice transcripts to be sensitive or not.

Although the services lack a proper definition of personal data, all of them reference data protection legislation in their terms. Hello Barbie, which is not currently available in Europe, promises to follow the regulations of COPPA, while Cayla and i-Que state that they

> *"are legally obliged to use the information in line with all laws concerning the protection of personal information, including the Data Protection Act 1998 and the Children's Online Privacy Protection Act (COPPA) of 1998 (together the "data protection laws")."*

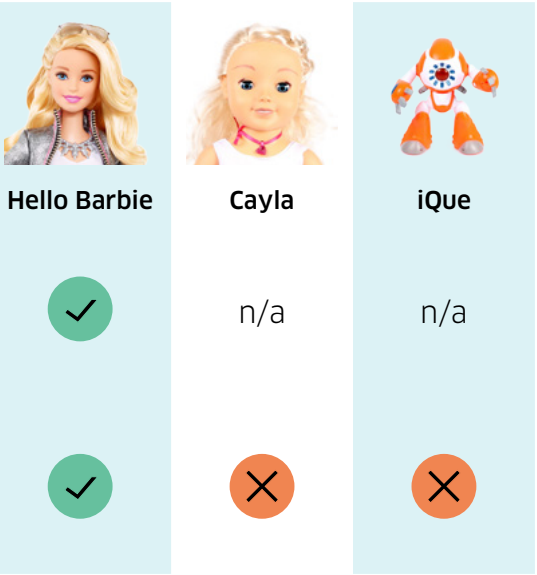
(Cayla and i-Que privacy policy)

This gives the user an indication that the service provider is committed to taking data protection seriously, although simply referencing "all laws" concerning these issues is unnecessarily broad. Giving a short but precise description of what they consider personal data, and how this data will be treated, would make it easier for the user to understand how their data may be used.

Data minimization

The principle of data minimization entails that services should not collect more data than strictly necessary in order to provide the service.[30] This principle is also reflected in European legislation.[31] This is important both because of respecting users' privacy, and because excess data collection may lead to unintended consequences through for example data breaches.[32] The relevant criterion here is that the services should limit data-collection to what is necessary for the functions of the toy.

6. Data minimization: Does the service limit the amount of required personal information to what's necessary to provide the service?



First, the NCC looked at whether the apps required the user to input any information upon installation. As mentioned, Hello Barbie has a parental control and verification system in place, meaning that parents have to register some information on an account before using the app. Only an e-mail address and password is needed for this, and a verification e-mail is sent to the submitted e-mail address before the app can be used. Additionally, the child's birthday can be entered through the parental account (presumably so Barbie can congratulate the child), but this is an optional feature.

30 https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/Glossary/pid/74 [accessed 21-10-2016]

31 Directive 95/96 article 6 b) and c)

32 In 2015, a data breach at the toymaker VTech exposed the personal data of millions of people, including many children. The leak included names, gender, and birth dates of children. This could have been less serious if VTech had limited the amount of children's data gathered. http://www.nytimes.com/2015/12/01/business/security-breach-at-toy-maker-vtech-includes-data-on-children.html?_r=0 [accessed 27-10-2016]

Cayla and i-Que does not have an account system, so no registration information is necessary before using the toys. However, their user agreements state that

> *"ToyQuest and its Licensors* ***may collect the contact names that appear in your address book*** *as part of the Services to tune, enhance and improve the speech recognition and other components of the Services****, and other services and products of ToyQuest and its Licensors."***

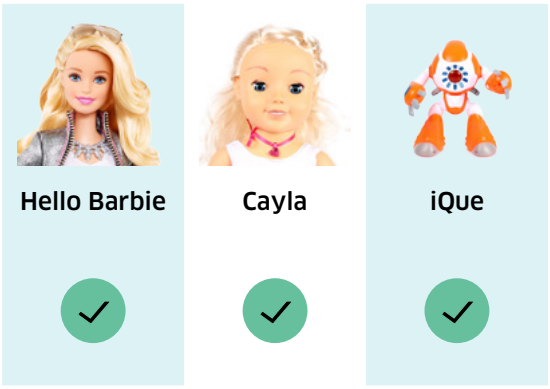
(Cayla and i-Que user agreement, emphasis added).

The NCC does not understand why ToyQuest or any licensors would need to collect their users' contact names for speech recognition purposes. This practice raises several privacy-related concerns. The contacts whose names are collected are unsuspecting parties, who have no way of knowing or consenting to their information being collected or used. "ToyQuest and its Licensors" is a very broad category, and "other services and products" means that these names could be used for almost anything, without specifying the nature of these "other services" at all. This is, in The NCC's opinion, a clear breach of the data minimization principle, and does not practice purpose limitation.

Permissions

When installing an app, it is important that the app does not ask for more permissions than necessary. This is another facet of the data minimization principle outlined above; the service provider should not request access to data that is not required for the interactive functions of the service. An of-cited example of requiring more permissions than necessary is a flashlight-app that required access to geolocation data.[33] The criterion set by the NCC is that permissions should be limited to strictly function-related purposes.

7. Permissions: Are the required permissions of the app necessary to provide the service?



	Hello Barbie	Cayla	iQue
The permissions are properly explained and justified	✓	✓	✓

33 https://www.theguardian.com/technology/2014/oct/03/android-flashlight-apps-permissions-privacy [accessed 08-11-2016]

The Hello Barbie Companion app requests access to files on the device, to storage, and to wi-fi. Both Cayla and i-Que requests access to files, the device microphone, wi-fi, and Bluetooth. Since Hello Barbie apparently does all recording in the doll itself, it does not request microphone-access. Cayla and i-Que needs access to wi-fi because they source information from the internet, while Hello Barbie uses a wi-fi connection to connect to the doll. I-Que and Cayla also need Bluetooth-access in order to connect the toys to the apps.

In other words, all of these permissions seem to be grounded and necessary for the products' main functions, thus fulfilling the NCC's criterion.

Purpose limitation – Sharing data with third parties

It is common for mobile apps to share user data with third parties, both for analytical and commercial (e.g. marketing) purposes. Since consumers should be able to assert some degree of control over their data, and make informed decisions when they consent, it should be possible to see who may receive user data. As a criterion, this should be provided through an accessible list of third parties, including the reason for why they are receiving user data and other information about the third parties' practices.

8. Third parties: Am I informed about who the service may share my data with?

The service makes it clear to me which third parties my data can be shared with

In their privacy policy, Hello Barbie and ToyTalk only state that they can share data with *"vendors, consultants, and other service providers"*, without specifying or giving examples of what this entails. As mentioned, Cayla and iQue's terms refers to licensors and third parties, and speech data *"shall only be used by ToyQuest and/or its* **Licensors or third parties acting under the direction of ToyQuest and/or its Licensors"** (Cayla and i-Que terms of service, emphasis added). Licensors and third parties acting under the direction of licensors is an extremely broad classification, and no information is provided about whom this may be. Additionally, if one was to locate these licensors or sub-licensors, informed consent would necessitate reading their terms as well, adding to an ever-branching tree of complicated documents. Although not an uncommon

issue, this illustrates the complexity and difficulty for consumers in even getting information about where their personal data may end up.

In the user agreements of Cayla and i-Que, the software-providers Nuance and IVONA are mentioned by name. These third parties may receive data when the toy is being asked a question:

> *"When you ask the App a question, this information request is stored on a Nuance Communication (for Apple-based users) or IVONA or Google (for Android/Google based users) server in the cloud. Collectively, Nuance and IVONA are our third party software partners ("Licensors")."*

(Cayla and i-Que user agreement)

The documents also specifically link to IVONA[34] and Nuance's[35] own privacy policies, encouraging users to read these *"For information regarding the privacy policies of our software partners"*. As will be elaborated upon in the section on technical testing, this is significant, as these third parties deliver speech recognition and text-to-speech technologies, meaning that they supply the interactive technologies used by the toys/apps.

In order to learn more about the policies regarding protection of speech data, then, one must also read the privacy policies for Nuance and IVONA. Although a complete analysis of these documents will not be done here due to considerations of length, a cursory overview of these companies' policies is in order. NCC thinks it is unreasonable to expect consumers to read not only the original terms and privacy policies, but also those of (often numerous) third party service providers.

Nuance Communications is an U.S.-based company specializing in voice- and speech-recognition technologies.[36] Since the i-Que and Cayla apps are part of their services, Nuance's privacy policy applies to any data (including voice data) that is sent from the apps to Nuance's servers. In addition to Genesis' already broad licenses to share and use data, Nuance adds a similarly wide scope, which includes the using personal data for marketing purposes:

> *"we may use the information that we collect for our internal purposes to develop, tune, enhance, and improve our products and services, and* ***for advertising and marketing*** *consistent with this Privacy Policy.* ***By using Nuance products and services, you acknowledge, consent and agree that Nuance may collect, process, and use the information that you provide to us*** *and that such information shall only be used by Nuance or* ***third parties acting under the direction of Nuance****,*

34 http://www.ivona.com/us/privacy/

35 http://www.nuance.com/company/company-overview/company-policies/privacy-policies/index.htm

36 http://www.nuance.com/company/index.htm?ref=footer

*pursuant to confidentiality agreements**, to develop, tune, enhance, and improve Nuance services and products.**"*

(Nuance privacy policy, emphasis added)

Note that by using Nuance's services, the user is assumed to have consented to Nuance's broad use of data.[37] Nuance may also share this data with even further unspecified third parties, making the roadmap of possible third parties increasingly obtuse, and further eroding the concepts of informed consent and purpose limitation.

Although Nuance's services are a part of Cayla and i-Que's companion apps, Nuance explicitly state in their privacy policy that their products are not directed at children:

"If you are under 18 or otherwise would be required to have parent or guardian consent to share information with Nuance, you should not send any information about yourself to us."

Nuance Communication privacy policy

Although it is unclear whether this is meant to apply to the particular use of Nuance's services in the Cayla and i-Que apps, the statement seems to be in conflict with the use of Nuance services in children's toys. Clearly children have little choice but to send their voice data to Nuance if they want to use their connected toy's interactive functions. They also reserve the right to record usage behaviour and IP-addresses without any apparent limitations:

*"**Nuance (or Nuance vendors and suppliers) may observe your activities**, preferences, and transactional data (such as your IP address and browser type) as well as related usage behavior depending on whether you are using our Website or a particular Nuance Product. **We may use this data for any purpose** unless we tell you otherwise in connection with a particular Website or product."*

Nuance privacy policy, emphasis added

Furthermore, if the user (or parent of user) has actually located and read Nuance's privacy policy, they still receive no guarantees that they will be notified if these terms change:

"If in the future we change our Privacy Policy, we will post the new Privacy Policy on this Website or Application. We reserve the right to

37 *"Nuance is the global leader in voice biometric solutions, with over 30 million enrolled voiceprints in the commercial space alone and numerous security-critical deployments. Nuance has developed unrivaled experience in delivering successful voice biometric solutions that enable military, intelligence and law enforcement agencies to ensure a safe and peaceful future for citizens."* (http://www.nuance.com/ucmprod/groups/enterprise/@web-enus/documents/collateral/nc_025785.pdf) [accessed 27-10-2016]

change this Privacy Policy in the future. Your continued use of this Website or Nuance Product following a change in the Privacy Policy represents consent to the new Privacy Policy to the fullest extent permitted by law. We encourage you to periodically review this Privacy Policy.»

(Nuance privacy policy)

In other words, in addition to regularly checking Cayla and i-Que's terms for updates, the user is also expected to periodically review Nuance's legal documents. If the user does not do this, their continued use of the companion app will nevertheless constitute consent. Additionally, even if the service experiences a security breach, they make no assurances that the user will ever know, stating that *"Nuance may post a notice on this website if a security breach occurs"*. As illustrated in the VTech-case, the breach of children's information is a serious concern, and in the case of such a breach, users should be notified properly, for example by e-mail or within the app interface.[38]

For Android-based users, IVONA is a Polish company owned by Amazon that provides text-to-speech technologies. It can therefore be assumed that their services are used by i-Que and Cayla in order to make the toys "speak" when gathering information from Wikipedia and the Weather Underground.

In other words, whereas Nuance provides the technology to convert user questions into text that can be used to search for answers online, IVONA's technology converts these answers (e.g. a Wikipedia article) into a voice clip that is played through the toy. In any such case, it does not seem like IVONA needs to receive any user data from the toys. It should be noted, however, that IVONA does not promise to notify users about changes to their terms, and like Nuance, they also recommend that users of their services should read the privacy policies of any (unspecified) third parties.

As a side note, although the Cayla and i-Que terms state that Nuance is used for iOS users, and IVONA is used on Android, the NCC's technical report found that the Android version transmits data to Nuance.[39] This seems to be a case of an error in the terms, since the actual services that Nuance and IVONA provide are materially different.

Purpose limitation - Advertising toward children

Although European regulation does not currently prohibit marketing towards children, there are strong restrictions guarding the interest of minors. Using

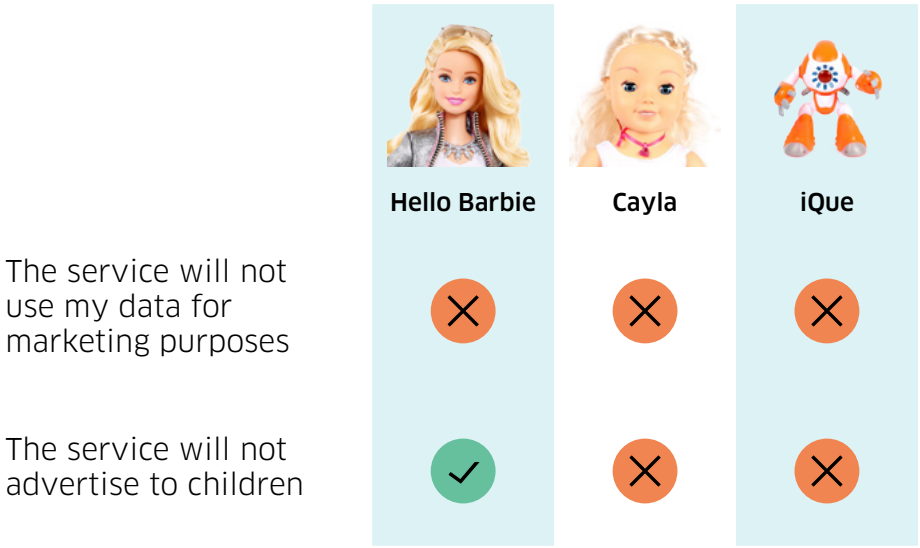
38 http://www.nytimes.com/2015/12/01/business/security-breach-at-toy-maker-vtech-includes-data-on-children.html?_r=0 [accessed 09-11-2016]

39 *Investigation of privacy and security issues with smart toys* (pp 11) – http://www.forbruker-radet.no/undersokelse/2016/toyfail-consumer-and-privacy-issues-in-connected-toys

children's data for behavioural and targeted advertising, which is tailored by analysing a large amount of data points, is especially controversial as younger and younger children are using the internet. By collecting data on these children, commercial third parties such as ad-brokers are able to create virtual profiles on which targeted advertising may be based.[40] Such advertisements may for example be displayed on websites, in other apps on the device, or even on other devices through the use of cross-device tracking technologies.

Based on this, the NCC looked at how the three toys position themselves in relation to marketing toward children. The criterion here was set according to the NCC's opinion that children should not be subjected to targeted advertising.

9. Advertising: Can the service use my data for marketing purposes?



Hello Barbie is very explicit about not using collected data in order to advertise to children. This extends to any third parties, including Mattel itself. However, they may use parents' information to advertise new products and services.

Cayla and i-Que's privacy policy tells a different story:

> *"Genesis may display* ***targeted advertisements based on*** *anonymised information,* ***personally identifiable information or information you make publicly available."***
>
> (Cayla and i-Que privacy policy, emphasis added)

This statement means that Genesis may base targeted advertising on any information collected through their services. They go on to state that "**by interacting with or viewing an advertisement you are consenting** *to the possibility that the advertiser will collect data from you*", which is problematic on several levels. As

40 For more on targeted/behavioral advertising aimed toward children, see http://www.enacso.eu/wp-content/uploads/2015/12/free-isnt.pdf [accessed 09-11-2016]

mentioned above, Cayla and i-Que also sends data to Nuance, who reserve the right to use personal data for marketing purposes.

Firstly, simply viewing an advertisement can hardly be considered explicit consent. Secondly, consenting to advertisers collecting data will potentially lead to more targeted marketing, which will lead to more data being collected, and so on. From the NCC's point of view this is clearly in breach of the principle of purpose limitation, since data collected for advertising is not a requirement for delivering the service. Especially since both Cayla and i-Que come with a significant price tag, it is, in the NCC's opinion, unreasonable to collect and monetize children's data as a continuous extra source of revenue.

Additionally, both Cayla and i-Que come with a large number of pre-programmed phrases, which also include a lot of reference to products such as Disney movies and Nickelodeon cartoons. The company behind the app, ToyQuest, have licensing agreements with several large brands geared toward children, including Disney and Nickelodeon.[41] When Cayla talks about how much she loves the Disney movie The Little Mermaid, for example, this can be a case of marketing within the toy. Hello Barbie, on the other hand, will happily talk about her friends and pets, who just happen to be separate Mattel products. This kind of product placement within the process of playing with a doll seems to be more or less uncharted territory, and may well be in breach of regulations on advertising toward children.[42]

Purpose limitation - Further use of voice data

Building further upon the principle of purpose limitation, the NCC looked at how the services reserve the right to use the collected voice data. While it is debatable whether it is ethically permissible to use children's voice data to enhance commercial voice recognition services, this could at least be argued to be a somewhat important component of the product and service (and it could improve the toy). However, if voice data is used for purposes beyond this, it is in breach of the purpose limitation principle. It could also be considered a violation of trust and privacy if the service shares children's conversations with their toys, or transcripts thereof, with unspecified third parties. Thus, the criterion is that voice data should not be used to improve services unrelated to the relevant toy.

41 http://www.toyquest.com/brands/brandsview/ [accessed 18-11-2016]

42 Unfair Commercial Practices Directive 2005/29/EC, chapter 2 and Norwegian Marketing Act chapter 4

10. Voice data: How does the service use my voice data?

	 Hello Barbie	 Cayla	 iQue
Voice data is not used for other purposes than to provide the service to me	✕	✕	✕

All three of the toys state that they may use voice data for analytical and research purposes. For Cayla and i-Que, ToyQuest reserve the right for themselves and their (unspecified) licensors to use voice data "**to tune, enhance and improve the speech recognition and other components of the Services, and other services and products."** (Cayla and i-Que User agreement, emphasis added). They moderate this statement by saying that these third parties will be subject to confidentiality agreements, but it still seems clear that by using voice data to improve other products, they are monetizing children's voice data.

Hello Barbie specifies that ToyTalk will not share voice data, but may still share transcripts with unspecified third parties:

> ***We may also share transcripts, text*** *or "feature extracted data" (which is data that is created from the voice recordings, but which no longer contain a child's voice), with service providers or* ***other third parties****, which they may use for research* ***and development purposes that are not rel ated to the services they provide us,*** *including developing, testing and improving speech recognition technology and artificial intelligence algorithms* ***not related to the services or technology being provided to ToyTalk.***

Hello Barbie privacy policy, emphasis added

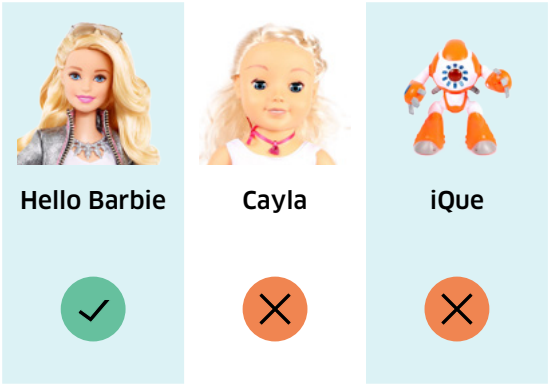
Although the actual voices are removed, the content of a child's interaction with their toy may certainly contain sensitive information that the child has shared with their toy in confidentiality. As with Cayla and i-Que, Hello Barbie also seems content to share sensitive data produced by children with third parties, who may use it for further commercial product research.

In the NCCs opinion, this is a breach of purpose limitation. As will be further noted below, this can also be considered a serious privacy issue, as children are deprived of their privacy through this sharing of data.

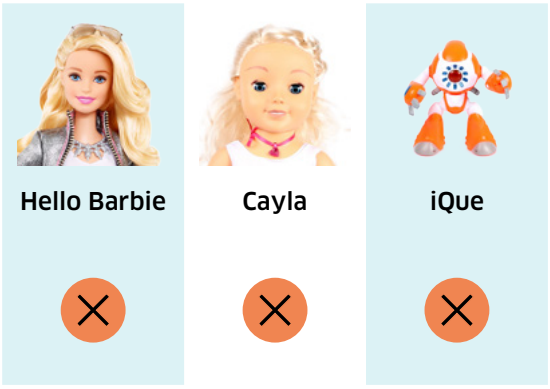
Data retention

Once data has been recorded by the service, it is also important that users can delete this information. This is grounded in the right to access and deletion, which is part of the EU Data Protection Directive.[43] Many users will delete an app or an account, and simply assume that their information is gone. In reality, this data will often be kept on the providers' and other third parties' servers for a long time, sometimes without any limitation at all. Additionally, if users become inactive, data should be automatically deleted after a certain specified amount of time. This is reflected in the Personal Data Directive, which requires a clear retention period.[44] Therefore NCC looked into how the privacy policies clarify deletion of personal data.

11. Data retention policies: Can I easily delete my data?



12. Data retention: Are my data deleted if I have stopped using the service or have been inactive for a while?



Hello Barbie promises that when a user account is deleted, all connected user data will be deleted as well. However, "cached copies may exist for a certain period of time" (Hello Barbie privacy policy). "A certain period of time" is very vague, and the user has no indication of whether this will be a month or five years. They also state that recordings may be deleted periodically from the

43 http://ec.europa.eu/justice/data-protection/individuals/rights/index_en.htm
44 Directive 95/46/EC article 6

parent account, "*but in such case, we may still have access to those voice recordings for research and development purposes*" (Hello Barbie privacy policy). In other words, ToyTalk may keep copies for themselves even if the parent no longer has access to voice clips.

Cayla and i-Que's privacy policies say that they will not keep personal information for longer than necessary, but without indicating what "longer than necessary" actually means. Since the same privacy policies also state that this data may be used for advertising, the timeframe of what is "necessary" could potentially be very wide, even perpetual. They go on to say that

> *"(…) it is not always possible to completely remove or delete all of your information from our databases without some residual data because of backups and other reasons"*
>
> Cayla and i-Que privacy policies

This is another case of very vague wording, and including "other reasons" practically puts no constraints on the reasons that the service providers may use to justify storing personal data. Finally they state that they may keep personal data for "legitimate business or legal purposes", extending the broadness even further.

Deleting an account

Whenever a user account can or must be created in order to use a digital service it should in the NCC's opinion not be harder to delete this account than it was to create it. This is closely related to the right to deletion, as users control of their data should extend to choosing when their data should no longer be retained or used. Although an account system is not always necessary, it can be useful for example in order to obtain verifiable parental consent, such as in the case of Hello Barbie. Thus, the criterion is that users should be able to delete their account in the same place as where the account was created.

Since Cayla and i-Que does not have an account system, they avoid this issue altogether. Hello Barbie's account system gives parents access to a dashboard where they can review recorded conversations, choose to share these with others, and to delete individual voice clips. Account deletion is also possible through this account.

> *"If you wish to stop any further collection or use of your child's personal information, or delete your email, you must delete your account from the Settings page."*
>
> Hello Barbie privacy policy

Although the deletion function is not available directly in the Hello Barbie app, the function is clearly linked to. This makes it rather straightforward for a parent to delete their account if they no longer want their child's data to be

recorded. As mentioned above, however, it seems like ToyTalk may still have access to voice clips after deletion. This is insufficient, as deletion means that all personal data should actually be deleted, and not just remove the user's access to their data. Insufficient removal of data could be a breach of the principle of purpose limitation.

Supporting the service

Unlike traditional toys, which can be played with until they physically break, connected toys are reliant on continuous support from the service provider in order to function as intended, with all their interactive features. Companion apps and web servers need to be updated and maintained, and if either of these services stop working, the internet-based functionality of the toys is practically broken.[45] On this basis, the NCC looked at whether the service providers promise or guarantee continuous functionality for the digital aspect of the products.

13. Support: Does the service provider say that they will keep supporting the service?

	 Hello Barbie	 Cayla	 iQue
The service does not reserve the right to shut down or otherwise remove my access to the service without a proper reason	✗	✗	✗

45 Products no longer functioning as intended because of lack of support is an emerging problem with the internet of things. The perhaps most widely discussed case of this happening was Google's smart hub Revolv, where all purchased devices were bricked when the service provider shut down the servers. http://www.forbes.com/sites/aarontilley/2016/04/12/nests-revolv-shutdown-debacle-underscores-business-model-challenges-for-internet-of-things/#5dddedb72add [accessed 28-10-2016]

All of the three toys reserve the right to stop providing the service at any time, and accept no liability if this happens. Hello Barbie's terms read as such:

> ***"ToyTalk reserves the right in its sole discretion to** review, improve, modify or **discontinue, temporarily or permanently, the Services, the Companion App and/or any features**, information, materials or content on or in the Services or the Companion App **with or without notice to you.** You agree **that ToyTalk will not be liable to you or any third party for any modification or discontinuance of the Companion App** or any portion thereof."*
>
> Hello Barbie Terms of Use, emphasis added

Similarly, i-Que and Cayla may stop functioning properly at any time, but limit the reasons for this to the following: "*technical difficulties, change of IT systems used to operate the App or violation by you of these Terms, or the Privacy Policy or the Appstore Rules.*" (Cayla and i-Que User Agreements). This is better than Hallo Barbie's disclaimer, but only marginally so, since the vague terms mean that a breach of the terms of service or privacy policy is hard to disprove. Notably, Hello Barbie's packaging has a disclaimer stating that *"We reserve the right to terminate the app service after 10-15-2018"*. Such a disclaimer on a children's toy may seem strange, but is most likely meant to disclaim liability, in addition to the financial cost of operating an app service with accompanying servers where voice clips are hosted. This might be problematic, since the discontinuation of the app service would directly impact the interactive functionalities of the doll, and toys with short lifespans could be a contributing factor to growing amounts of waste.

Termination from the service

As noted above, users may risk losing access to the digital portion of these connected toys, either because the provider stops supporting it, or because the user is "kicked out". In the latter case, the NCC's criterion is that consumers should be notified, and given a reason for the termination, so that they can contest the decision.[46]

14. Termination from service: Will the service notify me if my access to the service is terminated?

	 Hello Barbie	 Cayla	 iQue
The service will provide me notice if my access to the service is blocked or terminated	✗	✗	✗

Hello Barbie's terms of service state that

> *"ToyTalk may suspend and/or terminate your rights with respect to the Services for any reason or for no reason at all and with or without notice at ToyTalk's sole discretion."*

Hello Barbie terms of service

This is, in the NCC's opinion, clearly an unfair contract term, as the user has no way of knowing about or contesting the decision. It is especially grievous that the user's rights may be terminated "for no reason at all", meaning that ToyTalk may ban the user from using the Hello Barbie Companion app without reason, constituting an unbalanced term rendering the consumer with no real rights.

As mentioned above, Cayla and i-Que may also terminate user access without notice, which again gives the consumer no information of why they may have been banned. This is, in the NCC's opinion, a clear violation of basic consumer rights.

46 This could also be a question if the actual term infringes article 3(3) of the Directive on unfair contract terms in consumer contracts, cp annex, number 1, k - http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31993L0013

Technical testing

As a part of the analysis of connected toys, the NCC commissioned a technical test from the consultancy firm Bouvet.[47] Although the terms and conditions, together with other provided specifications, are the consumers' only real opportunity to familiarize themselves with the workings of the products, these do not necessarily reflect what is actually taking place. As an example, the NCC's earlier analysis of mobile apps revealed that the dating app Happn would share personal data with a third party, although their terms clearly stated that they would not do this.[48] In these cases, the user has no way of knowing that the service provider is breaching their own terms. The following section outlines the main findings of the technical tests, while more detailed results can be found in the attached technical report containing a complete account of the technical tests.

i-Que and Cayla

Background and method

During the technical testing of Cayla and i-Que, several aspects of the technology were examined, encompassing both the toy, the app, and the traffic between these and the internet. As mentioned, Cayla and i-Que function in similar ways, connecting to an app through a Bluetooth connection, and with the app fetching information from sources such as Wikipedia. Although both toys come with many pre-configured phrases and conversational topics, they use the internet to find answers to factually-based questions such as "Who is Barack Obama?". When this happens, the toy first has to recognize the keywords being queried about, which could prove to be a less than reliable process, as the voice recognition function is slow and inaccurate. Once the keyword is recognized, the app sends a call to Wikipedia containing the keyword, and returns with a (usually dry) answer that the toy recites verbatim from the relevant Wikipedia article.

Before a Bluetooth-enabled device can be connected to a smartphone or tablet, it has to be switched on and go through a pairing process. This is often done by having the user input a code, which is either randomly generated or printed on the IoT-device, on their phone/tablet. This code serves as an authentication mechanism, ensuring that only the owner will be able to connect to the device. In other cases, such a security mechanism can be reduced to having the user hold down a button in order to successfully pair the device and the phone/tablet, which means that physical access to both units are needed in order to establish a connection.

47 *Investigation of privacy and security issues with smart toys* – http://www.forbrukerradet.no/undersokelse/2016/toyfail-consumer-and-privacy-issues-in-connected-toys

48 http://www.forbrukerradet.no/side/happn-shares-user-data-in-violation-of-its-own-terms/ [accessed 28-10-2016]

Testing Bluetooth security

In the technical tests performed by Bouvet, they discovered that neither Cayla nor i-Que employs either of the aforementioned authentication mechanisms while pairing the Bluetooth devices. In fact, no security measures whatsoever seem to be implemented in the toys' Bluetooth-function. In practice, this means that anyone within a 15-meter radius (or somewhat shorter if connecting through concrete walls) can connect to the toys as long as they are turned on, and not already actively paired with another device. By simply turning on a phone's Bluetooth-function and pressing on the "IQUE" or "Top Toy Cayla"-prompts, the phone can be used to play any form of audio directly through the toy, effectively making it a Bluetooth-connected speaker.

According to the technical tests, the Bluetooth module implemented in Cayla supports the "Just Works" task flow, which means that users can connect without taking additional actions.

> *"The "Just Works" task flow is (...) useful whenever product implementers want to make the user experience easier and* ***have accepted the increased risk of security attacks****."* [49]
>
> Bluetooth Usability Expert Group

This seems to indicate that the manufacturers have accepted the risk of security flaws in order to make the user experience of connecting to the toys more seamless.

The unsecure Bluetooth-function also means that the toys can basically be used as a Bluetooth-headset. By connecting one phone to the toy through the unsecure Bluetooth, and calling that phone with a second phone, the testers were able to both talk and listen through the toys. This means that, by using two basic smartphones, anyone could potentially compromise the toys in order to both converse with and covertly listen to the owners. While the "listening" function is active, a light on Cayla's necklace and i-Que's "eye" activates, but this seems to be the only attempt at building any form of security into these products.

The issues outlined above are potentially very serious flaws for obvious reasons, especially since these products are likely to be kept in children's rooms and will be left turned on. These flaws are, however, not a new discovery. In early 2015, the white hat hacker group Pen Test Partners demonstrated these and several other security flaws in the Cayla doll.[50] The "hacking" of the doll garnered some media attention, appearing both in the BBC[51] and in the Wall Street Journal.[52] To the former, the UK distributor the Vivid Toy group stated

49 BLUETOOTH® User Interface Flow Diagrams For Bluetooth Secure Simple Pairing Devices https://www.bluetooth.org/docman/handlers/DownloadDoc.ashx?doc_id=86173 [accessed 07-1-2016]

50 https://www.pentestpartners.com/blog/making-childrens-toys-swear/ [accessed 28-10-2016]

51 http://www.bbc.com/news/technology-31059893 [accessed 28-10-2016]

52 http://www.wsj.com/articles/talking-toys-are-getting-smarter-should-we-be-worried-1450378215# [accessed 28-10-2016]

that this was "an isolated example carried out by a specialist team", and to the latter a representative of Genesis addressed these flaws by saying that the vulnerabilities had been fixed.

As the NCC's technical tests demonstrates, as of November 2016, neither of these statements are true. As a side note, the NCC notes that in 2016, Genesis released a new version of Cayla, called Party Time Cayla.[53] The unsecured Bluetooth module is still present in this new version, without any apparent attempt to remedy the security flaw. If the producers and distributors have been aware of these vulnerabilities since early 2015, the NCC considers this a serious breach of trust, as neither fixing or otherwise properly addressing the flaws could potentially put children in harm's way.

Data flow

Because of the already outlined wide licenses and rights granted to Genesis and ToyQuest regarding user data, the NCC were also interested in seeing what actually happened to the data in practice. In order to do so, a technical lab was set up to capture any data going out of and into the app through a wireless connection. A portion of the outgoing traffic that was observed consisted of calls to Wikipedia and Weather Underground as a result of questions being asked to the toys. These queries contained only keywords to be looked up, and the contents of the relevant Wikipedia-articles were sent in return. Presumably, the text-to-speech technology of IVONA is used in-app to convert these snippets into speech.

The testers also observed that the Cayla and i-Que apps uploaded data to an IP-address located in Burlington, Massachusetts. This is where the speech recognition service provider Nuance Communications has their main offices. Due to the size of the files, these encrypted data packages were assumed to be sound files including the user's voice. The terms of Cayla and i-Que acknowledge that data may be transferred to Nuance, and encourage the user to read Nuance's own privacy policy.[54] As outlined in the section on purpose limitation, this transfer of voice data is cause for some concern. Nuance reserve a right to share this data with other unnamed third parties, will not notify about data breaches, and say nothing about data retention periods. This makes it very difficult for users to give informed consent, as outlined in the previous sections.

Genesis themselves do not seem to receive any user data at all, in spite of what their terms and privacy policies seem to allow for. It is certainly positive if children's data is not actually being shared with the service providers, although this raises the question of *why* the legal documents flat out state that this data will be collected. Although it appears that the toys do not currently share any children's data, it remains disconcerting that Genesis reserve the rights to collect, use, and share such data for a wide array of purposes. Similarly, no data was found to be transmitted to the text-to-speech service provider IVONA.

53 http://www.myfriendcayla.com/cayla-partytime [accessed 07-11-2016]

54 http://www.nuance.com/company/company-overview/company-policies/privacy-policies/index.htm [accessed 08-10-2016]

Hello Barbie

In contrast to Cayla and i-Que, where a Bluetooth connection to the app is required for the app- and internet-based functions, the Hello Barbie doll connects directly to the internet through its own wi-fi connection. The companion app is necessary only when connecting to the doll for the first time, and a parent account has to be registered before using the interactive features. After the parent has registered an e-mail address, an e-mail is sent asking the parent to consent to the use of the toy. Subsequently, they can visit a "parent dashboard" to review, share, and delete any recordings made through the doll.

Like the other toys, Hello Barbie's terms also outline a rather wide potential use of voice recordings and transcripts. Although Barbie does not gather any information or answers from the internet, as all her dialogue is pre-recorded, voice data is collected to improve the services (and other purposes, as outlined above). The doll is able to answer some specific answers, such as "What is your name?", and is supposedly equipped to "remember" certain information.

Our technical tests found that Hello Barbie sends data to two IP-addresses based in San Francisco, where ToyTalk's offices are based. This connection is secured using SSL, meaning that the service uses encryption. The testing showed that these transmissions are made whenever the doll is answering questions, or uploading a recording. Although the tests could not establish the exact contents of these transmissions, it seems fair to assume that at least voice recordings are being sent. since the recordings are made available through the parent dashboard, which is hosted on ToyTalk's servers.

Product security in general is regulated through the General Product Safety Directive,[55] and toys are separately regulated in the Toy Safety Directive.[56] The Toy Safety Directive applies to *"products designed or intended, whether or not exclusively, for use in play by children under 14*.[57] Cayla, i-Que and Hello Barbie therefore fall within the scope of this directive. The directive specifically regulates toys' physical and mechanical, flammable, chemical, electrical, hygiene and radioactivity-related risks. The lack of digital security measures could, from a consumer perspective, constitute a potential weakness in the regulation of the security of toys.

55 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al21253

56 http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1479838714234&uri=CELEX:32009L0048

57 http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32009L0048

Other considerations

Children's privacy

The right to privacy is enshrined in the European Convention of Human Rights,[58] and further reflected in the European Data Protection Directive. Children's right to privacy and their particular position when it comes to privacy issues is reflected in several opinions from the Article 29 Working Group and the European Data Protection Supervisor.[59][60]

It is highly questionable whether functions such as Hello Barbie's allowing parents to share children's private conversations through Facebook respect this. Aside from the obvious security aspects, there is also an ethical side to these issues. Although these ethical considerations are otherwise outside of the scope of this report, they are worth considering when looking toward the future of the internet of toys.

It is worth asking whether children's speech data (or transcripts thereof) should be used for developing commercial products. If this is permissible, parents should at the very least have to give their explicit consent, rather than burying this point in the middle of the very long standard terms and conditions. Several actors have questioned the effects that "listening" devices could have on children's development.[61] [62] It could be argued that the recording of private conversation between a trusted "friend", is normalizing surveillance in unhealthy ways. Additionally, by sourcing answers to all sorts of questions from Wikipedia, Cayla and i-Que are able to present themselves as educational toys, but in practice they will often simply recite dry facts without context.

Security and the hacking of connected toys

As the IoT gains traction and widespread adoption, many security and privacy experts question the robustness of the networked devices.[63] Microchips and sensors are being implemented across a wide spectrum of physical devices, and are often cheaply made or manufactured without much apparent quality

58 http://www.echr.coe.int/Documents/Convention_ENG.pdf [accessed 21-10-2016]

59 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp147_en.pdf

60 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-07-17_Better_Iternet_Children_EN.pdf

61 *From the Beginning: Children as Subjects and Agents of Surveillance* http://web.mit.edu/gtmarx/www/childrenandsurveillance.html [accessed 21-10-2016]

62 *Surveillance Technologies and Children* https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2012/opc_201210/ [accessed 21-10-2016]

63 *How the Internet of Things will affect security & privacy* http://www.businessinsider.com/internet-of-things-security-privacy-2016-8?r=US&IR=T&IR=T [accessed 21-10-2016]

control.[64] As production costs and the physical size of these components are being reduced, it seems that many producers are neglecting security-issues to save on costs. As demonstrated by the technical testing of Cayla and i-Que, the use of cheaply made or simplified components can leave the IoT with serious security vulnerabilities.

Aside from lacking verification mechanisms or other basic Bluetooth-security, internet-connected devices without proper security measures in place may become vectors for targeted attacks.[65] In addition to cutting corners, many of these issues may stem from the simple fact that many of the manufacturers moving into the IoT have little or no experience with providing digital services. When traditionally analogue devices become connected, a new world of possibilities open up – not only for improved functionality, but also for serious vulnerabilities. Ten years ago it would be unthinkable that a children's doll could be used to perform targeted hacker attacks, and our findings suggest that the manufacturers have not prepared for these kind of scenarios. Although this issue is becoming increasingly significant for the entire IoT, it is especially disconcerting that products aimed at young children are failing to provide even basic safeguards.

Sexism in children's toys

These "intelligent" toys also embody the larger debate about sexism in children's toys. Hello Barbie is very interested in talking about clothes and toys, although she will also occasionally suggest career choices such as "politician". Cayla is happy to chatter about family, friends, and cooking, while the i-Que robot mostly steers the "conversation" toward science, lasers, and silly jokes.

The tendency of toys to push girls toward clothing and cooking, and boys toward science, is of course far from unique to these connected toys. However, the simulation of an actual conversation, which may seem very real to a child, may give these pre-recorded phrases an additional dimension of responsibility. Add the fact that Cayla and i-Que come with a "family filter", which apparently censors words and concepts including "gay marriage" in the UK version of the app, and it becomes clear that the "personalities" of these toys warrant a closer examination.[66] In our technical tests, it was also revealed that the Norwegian version of the apps has banned the Norwegian words for "homosexual", "bisexual", "lesbian", "atheism", and "LGBT", in addition to a bizarre list of crude words and controversial concepts.[67] Notably, the words "heterosexual" and "Christianity" are not on this list of banned words. This raises further questions about what kind of values these toys might veer children toward.

64 *For the Internet of things, the cost of cheap will be steep* **http://venturebeat.com/2015/01/10/for-the-internet-of-things-the-cost-of-cheap-will-be-steep/** [accessed 21-10-2016]

65 *Internet of Things botnets: You ain't seen nothing yet* **http://www.theregister.co.uk/2016/10/10/iot_botnet/** [accessed 21-10-2016]

66 **https://www.pentestpartners.com/blog/making-childrens-toys-swear/** [accessed 28-10-2016]

67 Other censored words include "menstruation", "scientology-member", "violence", "abortion", "religion", and "incest".
Note: This is for the Norwegian version of the app, and may be different in other versions.

Looking forward

In the course of this report, several different but often interconnected issues have been uncovered regarding these connected toys. On a hardware level, the manufacturers of Cayla and i-Que seem to have disregarded basic security measures in favour of making their devices easy to use. Looking at the terms and conditions of the toys, it has become clear that the service providers do not respect basic consumer and privacy rights. Voice data about children is collected without many seeming restrictions of whom this data might be shared with, and for which purposes it may be used. Through the technical tests commissioned by the NCC, it was revealed that the toys and connected apps share data with third parties, who come with their own legal documents that the consumer is expected to read. As noted, these third parties also come with their own set of disconcerting issues, illustrated by the chaotic and nearly incomprehensible tangle of legal documents that apply to them.

All of these problems are emblematic of the increased spread of internet connected devices and services. Using children's toys as a window into this interconnected world of devices and services offers key insights about concerns that become magnified since the intended users are young children. With this analysis as a basis, the NCC recommends several courses of action to remedy this worrying trend of disregard for consumer rights. Services should as a general rule conform to the principles of data minimization and purpose limitation. They should not collect more data than necessary for the functionality of the service, and this data should not be used for purposes that are not inherently required for these functions. Furthermore, as an increasing amount of manufacturers and service providers move into the digital field, they must be mindful of the new security and privacy risks that the digital world open up.

Another aspect to consider when dealing with connected toys, is that digital safety measures should be reflected in the applicable legislation on product security. The NCC questions whether this might constitute a lacuna in the legislation for product safety that should be sealed.

In order to prevent that these kind of issues keep surfacing, the NCC suggests that manufacturers of connected toys adopt a design-philosophy of privacy and security by design. This approach entails that privacy and security-related risk assessments are undertaken during the entire design-process, and that sufficient privacy and security measures are worked into the product design itself. This is also the way forward according to the European Commission and the Article 29 Working Party, and is codified in the new GDPR.[68] Considering possible security risks during the whole design-process not only makes the product more robust, it may also reduce the significant costs that are liable to arise as a result of discovering serious flaws after the product is already in circulation. It also brings the benefit of increasing consumer trust, which is especially important in cases regarding children's safety. In a growing market, it is essential that consumers, and especially children, are not being used as test objects for emerging and not properly tested products.

68 Regulation (EU) 2016/679 article 25 - http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679

Terms and conditions

Hello Barbie

ToS: https://www.toytalk.com/hellobarbie/terms/ [September 9, 2016]

PP: https://www.toytalk.com/hellobarbie/privacy/ [September 9, 2016]

My Friend Cayla

ToS: http://myfriendcayla.co.uk/agreement [not dated]

PP: http://www.myfriendcayla.com/privacy-policy [February 23, 2015]

I-Que Robot

ToS: http://ique-robot.co.uk/user-agreement [May 26, 2015]

PP: http://ique-robot.co.uk/privacy [February 23, 2015]

Nuance Communications

PP: http://www.nuance.com/company/company-overview/company-policies/privacy-policies/index.htm?ref=footer [December 2015]

Photo: Forbrukerrådet and Роман Magician

FOR MORE INFORMATION

Finn Lützow-Holm Myrstad
Head of section, digital services and electricity

E-mail: Finn.Myrstad@forbrukerradet.no
Mobile: +47 479 66 900