LK SHIELDS
YOUR LEGAL COUNSEL

TECHNOLOGY

The Internet of Things: Cayla doll is banned in Germany over privacy and security concerns

by **Peter Bolger**

The Internet of Things: Cayla doll is banned in Germany over privacy and security concerns

23rd February 2017 | by Peter Bolger

A connected doll (i.e. a doll connected to the Internet), ‘My Friend Cayla', was banned last week by Germany’s telecommunications regulator, the Federal Network Agency, as it classified the doll as an ‘illegal spying device’. Parents were also urged to disable the connected doll.

The connected doll, which was voted as one of the top toys by the Irish Times for Christmas 2014, provides children with a connected play experience by listening and talking to them. When connected to an app via Bluetooth, children can ask the doll questions. The child's speech is then converted into text using speech recognition software and the app then searches the Internet for the answer and responds to the child. The doll is essentially connected to the Internet and is an Internet of Things (IoT) device.

However, this connected doll has raised concerns about the potential threat to children’s data privacy as a child’s interactions with the doll are recorded and potentially shared with third parties, which may include sensitive information, such as a child’s secrets. There have also been allegations that due to an insecure Bluetooth connection embedded within the doll, hackers could listen in or even talk directly to children through the doll.

The complaints

In December 2016, privacy campaign groups in the United States submitted complaints to the US Federal Trade Commission alleging that a number of IoT toys (My Friend Cayla, i-Que Intelligent Robots and Hello Barbie) record children’s private conversations without any limitations on the collection, use or disclosure of this personal data in breach of data protection standards. The complaint also alleged that such toys could be heavily compromised because of an insecure Bluetooth connection.

Similar complaints were also made in the EU by consumer organisations to the European Commission, the International Consumer Protection and Enforcement Network (ICPEN) and to the European Data Protection Supervisor.

The EU complaints identified a number of issues:

Security – They noted that there are serious security flaws with two of the toys (My Friend Cayla and I-Que Intelligent Robots) as they have insufficient security measures to prevent unauthorised access to microphones and speakers.

Data Protection – They also claimed that the toys fail to meet data protection standards on a number of

fronts and gave specific examples:

- the companies behind these toys reserve the right to share children's personal data with unspecified third parties;
- the companies fail to properly identify or restrict the purposes for which they use and distribute children's voice data;
- the companies may use children's data for analytical and research purposes unrelated to the toys itself;
- children's data is collected and used for advertising purposes for which explicit consent has not been obtained;
- there are no clear data retention procedures in place; and
- companies request access to data which is not necessary for the functioning of the toys.

Consumer Protection – The complaints also alleged that these toys do not respect consumer protection standards and they identified a number of specific issues in this regard, some of which include:

- non-transparent terms and conditions; and
- pre-programmed phrases embedded within the toys which endorse specific ?commercial products, which constitute hidden product placement.

The Irish Data Protection Commissioner's Guidance Note on Connected Toys

The Office of the Data Protection Commissioner ("**ODPC**") in December 2016 issued a Guidance Note regarding possible data protection issues with toys that use microphones and cameras which connect to the Internet.

The ODPC cautions that any interactions a child might have with these toys is a 'potentially sensitive matter'. The ODPC highlighted, in particular, that some of these toys allow for the collection and recording of conversions between a doll and a child. It also warned that such voice recordings may be shared with third parties, for example for targeted advertising.

The ODPC has urged parents to take 'extra care' when buying these types of toys and has provided a useful set of questions for parents to consider before purchasing:

1. What kind of sensors does the doll come with, for instance can it record a child's voice, take photos or capture videos?
2. Can the toy connect to the Internet or use Bluetooth to connect to an app to access the Internet?
3. If there is an app available for use with the toy, can anyone download and use it?
4. Can the sensors and network connections be turned on and off? Do the sensors have to be activated by pressing a button in order for the toy to work? Is it obvious when sensors have been activated?
5. Is there clear information on how the sensors work and how you can control them?
6. Does the packaging or instructions make it clear that information collected may be sent across the Internet or to other third parties? If so, are the contact details for those third parties provided? Do those third parties have privacy policies allowing you to understand what they do with the personal data they collect?
7. Is it clear from the information provided that the information is being collected securely?
8. If you have to register on a website or open an account for the toy or the app, does it allow you to see what information is collected and enable you to request that such personal data be deleted, stop it being collected or stop it being used for things like advertising and other third party sharing?

Conclusion

While IoT creates new play experiences and learning opportunities for children, it also poses risks to their privacy and security as hackers may be able to gain unauthorised access and control of devices such as

connected toys. This highlights the need for connected devices such as toys to be designed with privacy, security and consumer protection laws in mind at the outset of the design stage, in order to avoid such issues arising at a later stage and also to avoid the cost of re-engineering products.

For further information on this topic, please contact Peter Bolger at pbolger@lkshields.ie.

About the Author

Peter Bolger
Partner

Peter is Head of our highly regarded Intellectual Property, Technology and Privacy team. He advises clients on all aspects of privacy law in respect of compliance, registration, international transfers, policies and audits including the GDPR.
T: +353 1 638 5877 **E:** pbolger@lkshields.ie