

Data Protection Commissioner - Guidance Note on Connected Toys

In 2016, the European Consumer Council contacted Data Protection Authorities around Europe to raise concerns regarding possible data protection issues that might occur when children and parents use toys with micro-phones and cameras that have an ability to connect to the internet. In October 2017, a similar notification¹ has been issued by the European Consumer Council regarding smart watches aimed at the children's market.

The toys, in particular dolls, may give the appearance of having a personality and human-like quality that appeals to children. In some instances, the toys can recognise words and react in certain ways which suggest an emotional response to what the child says or does. Some toys also connect to apps on smartphones or tablets. This might allow for the collection and recording of "conversations" between the doll and the child, or even act as a "walkie-talkie". For some of these products the voice recordings are shared with other companies, and the toys' terms and conditions may allow for your child's conversations to be used as the basis for targeted advertising.

Similarly, the smart watches in question allow parents to communicate with their child through a mobile-phone function, and to report the location of the child. An "SOS" button may be available to allow a quick dial capability if there is an emergency. However, it has been found that in some cases the communications functions are not secure and can be hacked allowing eavesdropping on conversations, or even direct communication with the child. The location function can also be manipulated by hackers to make the child appear somewhere else, and the "SOS" function can be tricked to use a non-trusted phone number.

Any interaction your child might have with these kinds of toys, smart watches or other similar smart devices is a potentially sensitive matter. Parents who are considering buying them this Christmas may wish to take extra care when selecting one that has a camera or voice recording ability, connects to the internet or allows remote connection using a smartphone or tablet app, or has a location tracking facility.

The things to look out for include:

- What kind of "sensors" does the toy or smart device have – for instance would it record your child's voice, understand certain words or phrases, take photographs, or allow video to be captured?
- Does it have GPS or other means to track location?
- Does the toy, or device, have an ability to connect to the internet or to use "Bluetooth" to connect to an app that you install on your smartphone or tablet?

¹ <http://www.beuc.eu/publications/new-research-reveals-alarming-security-flaws-smartwatches-children/html>

- If there is an app that you can use with the toy or device, can anyone download and use it or just kids (or parents) who have the device?
- Does a button on the toy or device have to be pressed, or does the toy have to be used in a certain way in order for the app to connect to it?
- Can you turn the other sensors, network connection or location tracking on and off, or does the child have to press a button each time in order for them to work?
- Is it clear to the child and to you when the sensors are working – for example, do the toys or devices light up or make a noise when the sensors are activated?
- When you read the packaging or manual that comes with the toy or device, is it clear how these sensors work and what you can do to control them?
- Does the packaging or instructions make it clear if the information is also sent across the internet to the manufacturer or any other companies or websites?
- Does the packaging or instructions say that the information is collected “securely” or using terms like “https” or “ssl” or “tls”?
- Where information is shared with others, are there contact details for these organisations? Do the companies’ websites have privacy policies that allow you understand what they do with the information they collect, how long they keep it for, and allow you to get in touch and ask that the information be erased?
- If you have to register on a website to open an account for the toy or the app, does it give you a “dashboard” or “portal” to see what information is collected and allow you to control it? (Specifically, can you request that personal data be deleted, stop it being collected or stop it being used for things like advertising/third party sharing?)
- Can you easily understand the terms and conditions and privacy or data protection implications of your child’s use of the toy or device and are you given the opportunity to consent to each purpose and to control the use of your child’s personal data?

If you find that the answers to these questions cannot be found or that you are not happy with them, then our advice to you is to think twice about purchasing the toy. If you are happy to buy the toy for your child, then take care to ensure that it is working in the way described, and that you are happy with what it is doing, especially when it shares information with an app or with companies or websites it might connect to.