GLOBAL 13.12.2017 | Jennifer Baker

Forget Big Brother, Tiny Tears is watching you

In an always-connected society, the internet of toys is the latest security concern

When I was 10, I desperately wanted a bright orange remote-controlled car for Christmas*. At the time it was the most futuristic toy I could imagine – no wires! – so it's easy for me to understand why children want the coolest, most high-tech toys available. But while many worry about the potential of the internet of things to be hacked, most parents haven't even considered the downside to the 'internet of toys'.

On the face of it, a hacked doll might not have the same potential for mishap as a hacked autonomous vehicle, but when toys are in the hands of the youngest in society, governments, standards bodies and manufacturers have an obligation to make them secure.

Last year, Forbrukerrådet, the Norwegian Consumer Council (NCC), conducted extensive research into the My Friend Cayla doll. The doll uses a Bluetooth microphone to collect information such as its young owner's voice, name, location and IP address, so it can interact. However, the unsecured Bluetooth device can easily allow strangers to listen or speak via Cayla.

German authorities banned the toy, deeming it to be a 'concealed transmitting device'. Meanwhile, the US Public Interest Research Group's annual Trouble in Toyland report, which looks at dangerous or toxic toys in the run-up to Christmas, listed smart toys as potentially threatening for the first time. Unsecured toys could be used not only to frighten small children, but to gain access to the property, or other devices in the home, making the whole family unsafe. And that's not to mention the vast amount of personal data that can be requested and stored.

Never switched off

We have grown used to an 'always-on' society. We can track our phones

when we lose them or see where the nearest available rent-a-bike is – and safety-conscious parents can buy wearables so they know where their child is at all times. The motivation is clear: parents believe such tracking devices will help them protect their children and ensure their safety. But what if parents aren't the only ones doing the tracking?

Research published last month by the NCC revealed how strangers can seize control of smartwatches that are targeted at children and use them as tracking and eavesdropping devices. Smartwatch marketing promises, among other things, that parents can be notified when their child leaves or enters a pre-defined 'safe' zone. However, the agency is worried that this could lead to complacency, thus putting the child at more risk.

'We question to what extent parents can actually be sure that the watches provide correct information about where a child is at all times. If, for example, the watches cannot specify 'safe' zones with 100% accuracy, the claims in the marketing can give parents a false sense of security that can potentially put children's safety at risk,' consumer ombudsman Elisabeth Lier Haugseth said. Many of the products tested by NCC also 'often disregard basic consumer and data protection rights', she added.

According to the report, because the data is transmitted and stored without encryption, a stranger could take control of a watch to track, listen to or communicate with a child. A hacker could also make it appear as though the child is somewhere else.

This year, the European Commission released a report on the internet of toys that included the phrase 'the datafication of childhood'. While physical threats are easy to grasp, we don't yet understand the ways in which constant monitoring and surveillance of children can affect them psychologically. For many of the smartwatches tested by the NCC, it is not possible to delete your data or user account.

Are parents in danger of infringing the privacy of their own children? Where do we draw the line between privacy and safety? That's a question for each individual family, but if they cannot trust the products, any balance they reach will be meaningless.

What can be done?

In March, the British House of Lords published a report recommending that the government and private actors such as internet service providers consider minimum standards for child-friendly design, privacy and data collection. The report also recommends doing more to teach children about internet use. 'It is no longer sufficient to teach digital skills in

specialist computer science classes,' it says. 'We recommend that digital literacy sit alongside reading, writing and mathematics as the fourth pillar of a child's education.

At European level, the Commission report also acknowledged that 'internet connected toys can offer new, important opportunities for play, learning, health and educational support, but they also raise questions about safety, security, privacy, trust and other fundamental rights of children'.

The EU urgently needs to regulate mandatory security standards for connected products, according to Monique Goyens, director general of European consumer rights group BEUC. 'Producers should immediately fix these flaws or they should find their products withdrawn from the market,' she says. 'Products that are connected to the internet are everywhere. Unfortunately, some producers seem to turn a blind eye to basic security and privacy standards in their rush to market such products. Market surveillance authorities should make sure that such products never reach the market in the first place.'

In the meantime, digital rights group EDRi has created a child-friendly booklet to help them make safer and more informed choices about what and how to share online. It includes chapters on what privacy is, how to use safer messaging systems and how to improve the security of smartphones.

**I did get the car, but it had stopped working by the second week in January...*



Jennifer Baker
Brussels

Jennifer Baker has been a journalist in print, radio, and television for nearly 20 years, the last eight specialising in EU policy and legislation especially in the tech/digital sector. Her aim is to translate EU policy-speak and tech jargon into understandable English. She likes good books and bad films.