When is a toothbrush not just a toothbrush?

FPS FORENSIC PSYCHOLOGICAL SERVICES
Supporting your Criminal and Civil Justice Needs

Joanna Adler looks into the fast-changing world of technology, connectivity and digital resilience. She writes this post in a personal capacity and tells us about a bluetooth enabled toothbrush for children, which raised a lot of questions about security vulnerabilities, protecting our privacy and data. Joanna is Professor of Forensic Psychology and Director of Forensic Psychological Services at Middlesex University. Her research is interested in violence, hate and safety and in young people's experiences. [Header image credit: Philips Communications, CC BY-NC-ND 2.0]

In November 2016 I bought an electronic toothbrush for a child, to encourage independent, effective tooth brushing. The child loves it, and oral hygiene has definitely improved. Twice daily, a parent turns on smartphone location and Bluetooth settings so that the brush app can interact directly with the toothbrush to show the child where to move it. These settings only allow the phone and toothbrush to 'communicate' with one another, but twice daily, there's that security vulnerability, from an app designed for children from age four. There are options to avoid the pairing entirely, but you lose personalisation. There are also options to commit this toothbrush fully to the internet of things, running it across all desired devices.

We like seamless connectivity, its convenience and ease. I wrote this post on 5 January 2017, and that morning there was an infectiously enthusiastic BBC report from CES 2017. Rory Cellan-Jones told us how much fun he was having doing yoga with a robot, and about the next step in those toothbrushes, where AI will power them to process personal data to improve our dental health. It also considered how far driverless cars have progressed. The BMW spokesperson enticed us with the idea that a 'smart home' could 'drive with you' – a film you started watching before leaving home could be played back to you in your car, which would automatically go into 'cinema mode', something that could legally happen for rear passengers already.

Protecting our privacy

Wearable technologies and digitally enhanced products can improve health and autonomy. Our real and virtual worlds are already meshing ever more smoothly, and that's what we apparently want. Even though I like the oxymoronic elegance of a smart dummy, and can appreciate the potential irony of using Barbie dolls to launch DDoS (Distributed Denial of Service) attacks, the internet of hacked things is not going away. It will impinge more on the services and parts of society that we care about, and neither industry nor governments seem to be acting with any kind alacrity to crack down on default passwords and to improve privacy, while most of the rest of us just like getting stuff for free.

Home About Around the world Publications Resources
Subscribe

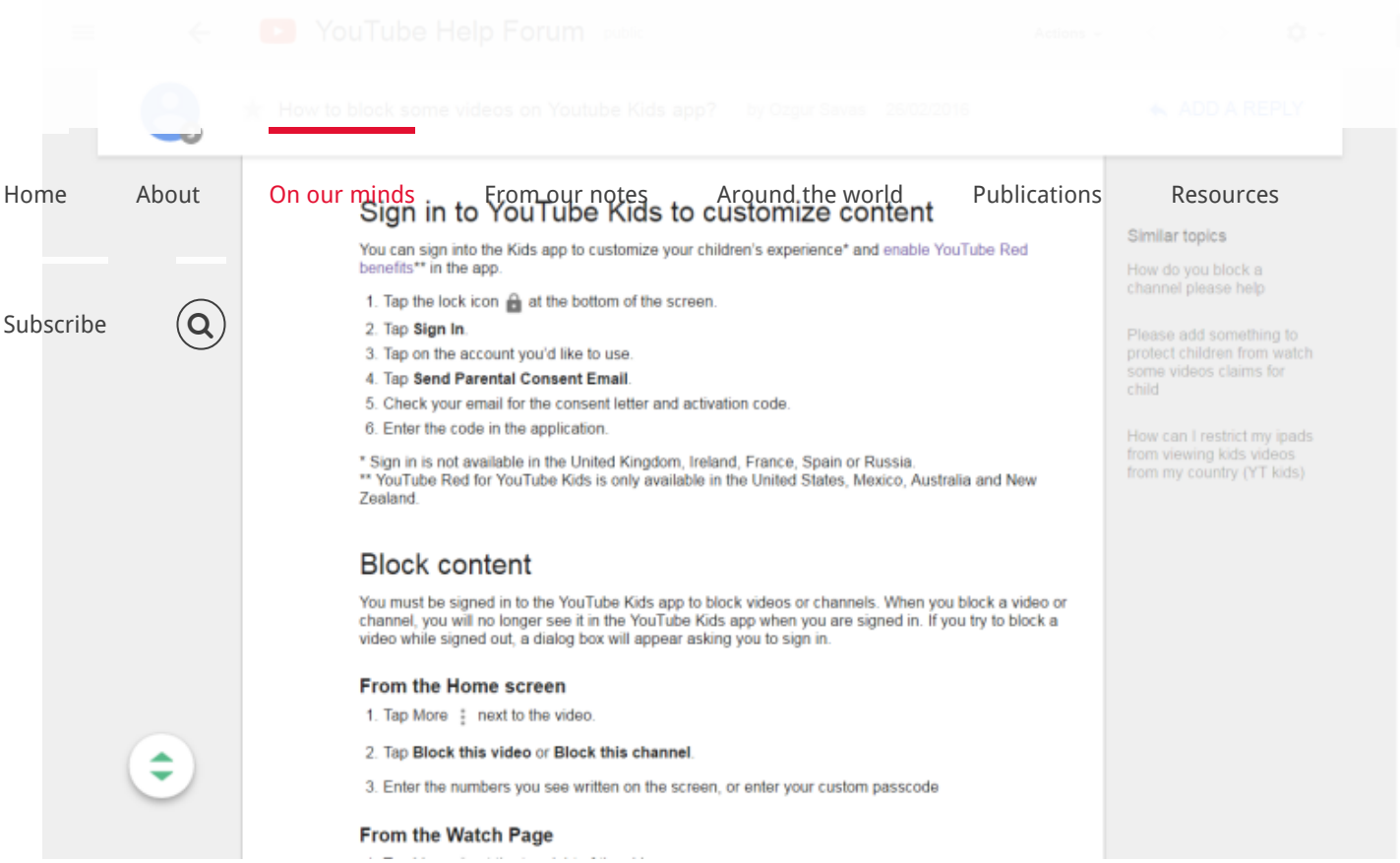
Our data

If we're not paying for something that costs something to produce, how is it funded? We're the data. Ad-tracking and algorithm-based filtering are based on our choices, but are not neutral. We pay for all the stuff we like to access or own 'for free', through our privacy, our preferences and those of our children – data from phone beacons, search engines, streaming selections, the outcomes of conscious and non-conscious decisions that we make on devices and that we pass on, time and again, without thinking. The extent to which that's a problem depends on who is getting data, about whom, the security of data, the extent and efficacy of anonymisation, the uses to which the data are put, whether or not users have genuinely chosen to pass on such data, whether or not they are legally empowered even to consent to their data being used in such ways, and the impacts this all has on us. These questions are all raised by the implications and enactment of the General Data Protection Regulation (GDPR).

Ad blocking

The Children's Commissioner for England has also recently added her voice to concerns about the advertisements served up to children and young people, noting that they often can't tell when something is an ad. This chimes with wider concerns about children's media literacy. So what about ad-free sites? Paid-for subscription services are one way to proceed, but they are only available in certain jurisdictions and exclude those who can't or won't pay for the services. We can use ad-blocking software on free services, and if everyone used ad blockers, that really would disrupt the internet business model. But how likely is it that we're all going to embrace an approach that means we start paying for things we think we're currently getting for free?

Google are quite proud of YouTube Kids, and tell us that it's more responsible, a place for under-13s to browse safely with a professed family-oriented advertising policy, which is freely available. It has two 'prohibited' sets of advertising – the first is 'restricted', which is apparently not as 'prohibited' as the other set, which is 'strictly prohibited'. Both only pertain to adverts directly paid for with Google: 'Content uploaded by users to their channels are not considered Paid Ads.' But that's okay, because if there's a really annoying channel that keeps popping up, like a pre-school child reviewing toys, we can use parental filters and block channels that we don't want children to see. Ah, no, apparently not in the UK. Maybe our legislation hasn't made that a necessary operating principle.



A new social contract

That's the nub of this problem: legislation will never be as swift or as agile as exponentially developing technology. However, if legislators abrogate their duties, there can be no commercial incentives to act more ethically, and there won't be independent scrutiny. That is why both the Digital Economy Bill and the GDPR are so important, but also why each may be insufficient.

A new social contract and regulatory framework for the rapidly evolving digital ecosystem require us to play our parts too. I have highlighted YouTube Kids here, but pick any major player you like. None of them should be expected to be our personal ethical filters, and we can't abrogate parental responsibilities to any entity that has its own duties to employees, shareholders or trustees. The Children's Commissioner's report suggests a digital ombudsman to mediate between young people and social media companies, although the scope and remit of such a role is not entirely clear. The report also pushes forward the 5Rights for young people and calls for a joined-up programme to build digital resilience through digital citizenship. It joins calls to review the UN Convention on the Rights of the Child to include digital rights and protections.

This is ambitious and makes sense, but as with real-world rights, these measures can only offer protection if they are implemented and if we all understand their consequences, both when flouted and when enacted. Meanwhile, maybe we could think a little more before turning on location settings, and if an internet of things device has an unchangeable password, it won't be getting room in my bathroom cabinet anytime soon.

January 11th, 2017 | Featured, On our minds | 0 Comments