EXPLORING THE RISKS OF CHILDREN ENGAGING WITH PROGRAMMABLE IOT

Sophie Beck[1]*, Bran Knowles[1], Joe Finney[1]

[1]School of Computing and Communications, Lancaster University, Lancaster, UK
**s.beck@lancaster.ac.uk*

Keywords: INTERNET OF THINGS, BBC MICRO:BIT, PRIVACY, SECURITY, ETHICS

Abstract

This paper reports on IoT4Kids, a study exploring the privacy, security and safety implications of children programming the Internet of Things. The study focuses on the BBC micro:bit as one device that allows children to create rudimentary IoT devices. Prior publications have described the first stage of this study, which involved workshops with child participants. This paper instead focuses on the second stage of the project, which involved conducting key informant interviews with representatives from our project partners in order to understand the risks children face with interacting with programmable IoT devices. We describe themes that emerged from these interviews, along with implications for the study and for future work in this area.

1 Introduction

The BBC micro:bit was developed in response to government priorities of increasing computer literacy among children [1.2], with the BBC seeking to launch a product to help children learn physical computing skills by engaging in building IoT devices. This initiative was driven in recognition that other maker tools on the market (e.g. Raspberry Pi and Arduino) can be difficult for novices to use, hence the micro:bit's developers aimed to lower the threshold for programming so that such tools were accessible to children without coding being the essential goal of their making activity.

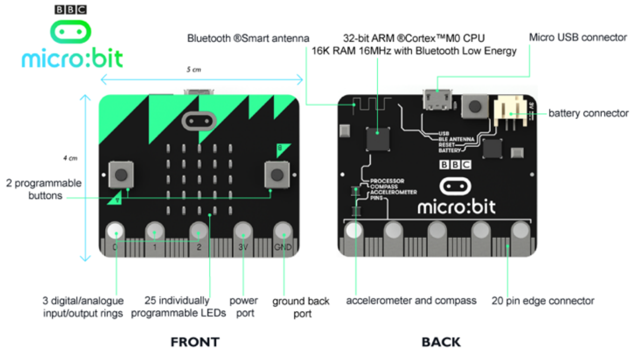

Figure 1: The BBC micro:bit.

Due to privacy and security concerns that may arise in the context of programmable IoT for child users, the micro:bit's developers decided to limited some of the functionality that makes it an IoT device, though the ambition remains to launch the tool with full IoT capability following more thorough risk assessment process. The PETRAS funded Iot4Kids project was inspired by this need for greater understanding of the risks associated with the BBC micro:bit specifically, and with IoT technology for children more generally. Working in partnership with The Family Online Safety Institute (FOSI), the National Society for the Prevention of Cruelty to Children (NSPCC) and the Micro:bit foundation, the project aimed to identify current and anticipated risks associated with the micro:bit and similar devices aimed at children in order to understand how to effectively mitigate against these risks.

In this paper, we focus on the second stage of the IoT4Kids project – after we had collected data about what devices children would likely use the micro:bit to create, identified different categories of use and potential risks therein, and translated these into risks into provisional Use Scenarios. Here, we report on the feedback we received from our project partners regarding the findings from this prior stage. We describe how interviews and a Knowledge Exchange workshop informed a more rounded understanding of the types of abuse children are susceptible to and the ways in which such abuse may be facilitated by IoT technologies. We also describe the various considerations by The Micro:bit Educational Foundation in developing the BBC micro:bit, and how these risks were mapped against certain features of the tool. Finally, we end with our thoughts regarding a guiding philosophy for safeguarding children from IoT risk – what we have dubbed 'learning to fall safely' – and potential directions forward in a multipronged strategy for realising safe IoT.

2. Methodology

2.1 Project overview

The IoT4Kids project comprises three stages. In stage one, 57 children (ages 9-11) were invited to take part in Outreach Days, where they explored how they might wish to use the BBC micro:bit [3]. They were guided through a creative exercise to elicit sketches and descriptions of their ideas for devices they would want to build. Analysis of this data was used to identify three categories of use (Assistance, Companionship and Play) within which different clusters of risk emerge. These risks were elaborated in the form of Use Scenarios, i.e. fictional amalgamations of the participants' designs, crafted to illustrate emerging privacy and security implications of children's likely interactions with the micro:bit.

We focus in this paper on stage two, where we sought to bolster the use scenarios with information gleaned from our project partners. The National Society for the Prevention of Cruelty to Children (NSPCC) and the Family Online Safety Institute (FOSI) provided expertise in predatory behaviour to help us anticipate threats to children; and The Micro:bit Educational Foundation provided information regarding the necessary tech components and skills for realising children's desired uses of the mirco:bit, as well as known uses of the tool by children to date. Feedback was solicited from these project partners in order to further refine and expand the set of Use Scenarios.

In stage three, the resulting Use Scenarios were then used as a basis from which to derive questions that should be asked to help mitigate against the risks identified in the scenarios. These questions were categorised into four Risk Zones: 1) Authority and Discipline; 2) Malevolence and Accidental Harm; 3) Emotionality and Socialization; and 4) Governance and Accounting. These Risk Zones and guiding questions therein comprise our Risk Mitigation Checklist, a tool to be used by developers and policymakers to anticipate and proactively attend to risks of IoT technologies [4].

2.2 Details of stage two

We conducted five interviews with six participants. Participants were drawn from project partner organisations: five were from The Micro:bit Educational Foundation, the consortium of organisations that developed the BBC micro:bit; and the other one was drawn from our project partner FOSI. The goal of these activities was to better understand the risks children might face when interacting with programmable IoT devices. Specific objectives were to:

- better understand predatory behaviour and online safety risks for children;
- map these risks to components of the micro:bit to understand barriers to responsible deployment of this tool and others like it; and
- generate insights to help us refine and further develop the use scenarios produced during stage one of the project for use in stage three.

Semi-structured interviews with representatives from The Micro:bit Educational Foundation focused on the barriers faced by the development team during the process of designing the BBC micro:bit and surrounding infrastructure, and what they felt needed to be in place to ensure its responsible deployment for child users. Semi-structured interviews with representatives from FOSI focused on known predatory behaviour as it pertains to online safety, and concerns regarding risks to children arising from IoT technologies. All interviews took approximately 1 hour. The use scenarios were sent to the participants prior to the interviews and were used as discussion points to lead the interviews.

The interviews were recorded using a Livescribe Smart Pen. During the interviews key words were jotted down in the Livescribe Dot Paper notebook to provide quick referral back to interesting interview content. Immediately following interviews, the researcher conducting the interviews captured notes relating to initial insights. The interviews were transcribed and reviewed to heighten familiarity with the data. The transcriptions were then coded for emerging themes using the comments function in Microsoft Word. Post-It Notes were used to help organise these themes as they emerged.

Also contributing to stage two, a Knowledge Exchange Workshop was held in order to solicit feedback on the initial Use Scenarios and gain insights into predatory behaviour. Four Participants agreed to attend, whom were responsible for child online safety policy and guidelines. The research team travelled to the NSPCC headquarters for the 3-hour workshop. Prior to the workshop the NSPCC attendees were emailed the use scenarios, along with participant information sheets and consent forms. This allowed the participants to familiarise themselves with the scenarios beforehand and highlight any areas of concern or recommend changes to the scenarios.

Regular team meeting were held in order to discuss the findings from the interviews and workshop and the emerging themes.

3 Results

3.1 Types of abuse and risk

The Knowledge Exchange workshop resulted in a clear articulation of different types of child abuse that are worth considering in the context of children's online and IoT interactions. The first is *unknown adult abuse*, which is when "somebody who doesn't know the child contacts them online and then proceeds to develop a trusting relationship with them and then it leads onto abuse" (P2, NSPCC). This kind of abuse fits with traditional notions of 'Stranger Danger', which may happen either online or offline.

The second form is *known adult abuse* – i.e. abuse by family members, teachers, coaches, etc. – which is significantly more common: "90% of abuse happens within the home, so actually when we are talking about abuse and neglect, quite often it something within a family circumstance" (P2, NSPCC). P2 went on to say, "Then there's grooming by a known adult that could be say, a sports coach, that develops a relationship with a child and then they are using technology to facilitate that, because the big thing is the big benefit but also risk is with all this online technology is that it provides very private mechanisms for communication, that just would not have existed in any other face to face, telephone type of communication, like from 30 years ago."

The third form is *peer-to-peer abuse*, which is often not recognized by the victim in the early stages, but is characterised by "cohesion, control and manipulation" (P2, NSPCC). Peer-to-peer abusers can utilise technology in order to facilitate the abuse, gaining the trust of the victim and then manipulating him/her.

Up until this point, our thinking had focused largely on the less common unknown adult abuse, i.e. predators making contact with and grooming children [5]. This may be because of the recent headlines regarding, for example, the use of Minecraft forums by pedophiles [6]. The interviews further generated a number of more specific concerns to guide our research. These included cyberbullying, data protection, inappropriate marketing, inappropriate content, mental health, radicalisation and health & safety.

3.1.1 Cyberbullying: FOSI and other child advocate groups highlight the concerns of online bullying or cyber bullying. Approximately 1 in every 8 children have experienced bullying on social media [7]. Cyber bullying can be widespread and facilitated through social media. It is defined as the use of the internet and digital technologies in order to tease, threaten, upset or humiliate someone [8].

3.1.2 Data protection: The General Data Protection Regulation (GDPR) provision relating to children's data seeks to enhance the protection of children's personal data as well as ensuring that companies explain clearly to young people what data is being collected, and how it is stored and used. A child is classed as anyone under the age of 18 [9]. Social network sites do specify a requirement of 13 years of age in order for consent during the sign up to the service [9], but in reality "almost 1 in 4 of 8 to 11-year-olds and 3 in 4 of 12 to 15-year-olds" [7] have some form of social media profile.

3.1.3 Inappropriate marketing: Individuals are exposed to a myriad of advertising campaigns when online. Younger people may not have the same capacity to filter this information, which is why marketing to children requires additional ethical consideration. Children's data may be used for marketing purposes, however the GDPR "makes clear that any marketing must be fair and not exploit the vulnerability of children" [10].

3.1.4 Inappropriate content: As more children watch and engage with online materials, the risks associated with viewing inappropriate content has increased. Traditional means of viewing visual content via television channels were vetted and curated via corporation responsible for broadcasting. There have been instances of children accessing inappropriate content disguised as their favourite cartoon characters via YouTube. Our informants explained that it is a widely held assumption by parents that YouTube is the same as watching BBC, with many abdicating responsibility for overseeing viewing, thinking "it is doing something, when actually it is not doing what you think" (P2, NSPCC).

3.1.5 Mental health: Studies in recent years have begun to link the wide spread use of online platforms and social media to negative mental wellbeing, in particular to reduction in self-esteem and healthy self-image [11]. The use of technology within the context of competitive sports was highlighted as a concern in the interviews, as it was seen to promote constant monitoring of personal activity (e.g. step counters). This was seen to potentially exacerbate behavior related to eating disorders; and there was potential risk of such data being leveraged for known adult abuse, e.g. a sports coach telling an athlete "you have not run far enough" (P4, NSPCC).

3.1.6 Radicalisation: The Internet is one of the most effective means to spread extremist ideologies and promote terrorist violence, which is why schools now include elements of online safety education pertaining to radicalization. But we note, "In reality the radicalization of children is rare and particularly nuanced, and far from a linear process that exclusively occurs online" [12].

3.1.7 Health & safety: Interviews with the Micro:bit Educational Foundation revealed that health and safety risks influenced the design of the BBC micro:bit, e.g. when considering how it was going to be powered. While such risks were mitigated in the design, our key informants noted that most of the health and safety risks emerge as a result of the build process itself, e.g. creating devices that could inflict intentional or unintentional physical harm to others.

3.2 Linking risks to desired uses of the BBC micro:bit

Having elaborated the types of abuse and risk (above), we describe below how these risks pertain more specifically to the contexts of use for the BBC micro:bit that emerged from the participants during stage one of the project (detailed in [3,4]).

3.2.1 Two-way communication: Many of the designs sketched by children in the Outreach Days from stage one involved some form of two-way communication. This may be attributed to children becoming familiar with technology such as Hello Google, Siri and Alexa. Key informants from The Micro:bit Educational Foundation explained that they recognised early on that enabling communication was essential functionality for a tool that children would want to use. There are three ways such communication could be achieved, each with different degrees of risk.

Wifi was deemed by our key informants to hold high risk, despite its undeniable appeal for opening up communication opportunities. Concerns were principally rooted in existing known risks pertaining to online safety, e.g. the ways in which various forms of grooming are facilitated by online interactions. For this reason, the micro:bit's developers focused on Bluetooth and Radio communication as a mechanism for two-way communication.

Bluetooth was a particular concern during the development of the BBC micro:bit. Though originally designed in as a way of enabling two-way communication, concerns over what information was being received by the other device it was paired to prompted developers to temporarily restrict Bluetooth. Specifically, developers were concerned about the device beaconing out its mac address, which might be intercepted by someone 30 metres away (unknown adult abuse risk). But additionally, whilst children might have found it 'fun' to send anonymous messages, the development team expressed concerns regarding bullying and not being able to identify the sender of the message (peer-to-peer abuse risk).

As our key informants explained, a custom radio communication component was designed in order to mitigate the tracking risks of Bluetooth, whilst still having a functionality that would inspire children. Most devices have an identifier, but this radio does not and therefore all data is sent anonymously. There is no source address and no destination address; children can share simple messages and commands within a closed space (e.g. the classroom) without revealing identifying information. Our informants describe their approach as one of making data non-personal and focussing on the data rather than the sender.

3.2.2 Personal or sensitive data collection and storage: Key informants revealed that consideration of data collected through the micro:bit played a vital role in shaping the device and the development of supporting platforms. One participant highlighted that during the BBC micro:bit development "We did start to look at this, if you're looking at the micro:bit itself as collecting data that seems fine, it's the step where you take the data off the micro:bit and then store it, you know apart from the obvious ones, which is who has access to that data, where is that data stored, then this is leading to all the data security stuff"(P9, Micro:bit Educational Foundation).

Developers were cognizant that what seems like innocuous data can actually become very sensitive and put children at risk. With the case of the micro:bit great consideration was taken to ensure data collecting and transmitted remained non-personal and could not be identifiable to the child. When children were to start to build devices which included cameras and microphones the risks increase, with additional forms of data that may inadvertently identify a child. IoT devices were noted for their ability to transmit very intimate data: "data knowing when someone is moving, when someone is stationary, I mean obviously if it is a bed, you know when someone is sleeping, then you have concerns around general safety" (P1, FOSI).

Storage of personally identifying data was also a concern from the outset for the BBC micro:bit's developers. The GDPR outlines that organisations need to have transparency and accountability when it comes to handling children's data [13]; and high profile failures of IoT toys such as the My Friend Cayla doll [14] made clear how important it is to protect against hacking, and how such hacks could have far reaching consequences both for the safety and privacy of the child and for the reputation of the company.

3.2.3 Surveillance: Designs generated by our child participants in stage one revealed that children frequently imagined devices with some form of tracking or surveillance. Notably, they did not express any concern over tracking or being tracked. One participant (P4, NSPCC) who had attended one of the IoT4kids Outreach Days in stage one expressed having been "really struck by how relaxed" children were in coming up with concepts that enabled parents could use the technology as a mechanism for discipline through surveillance. Our NSPCC informants noted that surveillance devices are and could be used for more malevolent purposes within the home (i.e. known adult abuse): "If you are a parent or uncle or someone who is abusing a child, if you could have one of these micro:bits in a room and you could be like, 'If you tell anyone I am going to know,' things like that. It's like you have put on that additional layer, you have the shame, you have the fear, you have the not really knowing what is going on but you also have got that thing that you have got no privacy whatsoever, that you can't talk about these things" (P2, NSPCC).

The covert nature of devices was seen by our key informants as another potential area of concern. The BBC micro:bit development team had considered apps which would link to phone cameras via Bluetooth to take 'selfies' in order to appeal to young people, but "child protection was concerned about people placing the phones and then them being able to remotely use them, and then taking videos with no sound" (P6, Micro:bit Educational Foundation). In order to reduce the risk, the development team considered an alarm that make sounds when the picture was taken. The team was also cognizant of risks associated with microphones, as in prior cases of security flaws with connected toys in which private conversations were recorded and then easily accessible by hackers [14].

3.2.4 Infrastructure Provision: A number of the children's designs from stage one entailed creating some form of profile. Concerns were raised regarding a potential lack of understanding on the part of the child about what data is being collected and where their data is going, and therefore what the risks are that they are entering into. Participants noted in particular the lack of trusted organisations with which a child might create a profile. According to one participant, "The child could build [a device] taking safety precautions and telling their parents everything about the device, but if they upload the data with the best of their intentions onto a website and then they could have data breach, because then that data is out there, and it can't be taken back".

Key informants explained that they had considered developing platforms for children to upload their data, but that the risks and costs associated with building such platforms were deemed too high, e.g. risk to organisational reputation if sensitive data was stolen. Informants suggested the need for a mixture of child education, adults overseeing activity, and trusted sites. Specifically, children would need to be guided to sites that meet "certain standards, then safeguarding and government safety standards" (P4, NSPCC), where the parents or guardians could tell their children "You are only allowed to download code from this site and if you get code from that site it is dangerous" (P4).

4 Discussion

4.1 Adult responsibility and safe play

In its current state, with radio communication and Bluetooth pairing functionality restricted and with its use being limited to safe (closed) environments, the BBC micro:bit poses effectively zero risks to children. The tradeoff is that its potential is severely limited: "you could lock the whole system down so that it becomes a pointless education system and kids could be learning nothing, or you can start to open that up to a point where they will start to learn stuff and even about the security, but of course when [you] do that they become more and more insecure" (P9, The Micro:bit Foundatio). Moreover, locking this one device down does nothing to prepare children for safely navigating the wider world of IoT devices that they are likely to encounter, most of which will not have been designed with such a clear ethical imperative and focus on vulnerabilities of child users. What would an approach look like that sought to prepare children to interact safely with the full range of IoT technologies they could encounter?

The metaphor of a playground might be instructive here. A playground is a space designed specifically for safe play: "Both social, emotional and physical risk happen in play, what we tend to do around play is to put enough stuff around to say that the emotional, social and physical risk within that [can be] managed by an adult" (P9, The Micro:bit Educational

Foundation). Our initial approach to this project, and the approach taken by the BBC and The Micro:bit Educational Foundation consortium in developing the micro:bit, was to design a digital playground: a safely constructed, gated space for children to play and take risks, "to experiment… with emotional, social and technical constructs that they are going to have to deal with as adults," (P9) under the supervision of parents, carers or teachers. The risks to the child in the digital playground are minimized as long as a) the adults supervising the play are sufficiently knowledgable of "the potential implications of what [the children] get up to" (P1, FOSI), b) these adults are vigilant and ever present, and c) the children do not venture out of the playground.

Consider instead an alternative strategy that is less demanding of those in supervisory roles and allows greater freedom for children to explore the world beyond the gate: namely *teaching children how to fall safely*. On a playground, the risks of falling are literal, and there are techniques that can be taught for falling safely, such as crouching, relaxing one's body, landing on fleshy parts of the body rather than putting hands down, rolling. In the digital realm, we mean 'fall' metaphorically, as in doing something that could result in harm. What would children need to know to be able to fall safely in the world of IoT?

4.2 Directions going forward

Our findings appear to imply the need for a multipronged strategy for mitigating risks to children. We identify four areas where effort may be focused.

4.2.1 Industry: The BBC micro: bit was developed with a clear imperative to protect child users. Ideally other companies would take this approach, carefully considering the risks to children as they develop their products. It may be beneficial to formalise this process, e.g. developing a framework that enables companies to progress through a series of relevant considerations. We have attempted to provide a start for such a framework with our Risk Mitigation Checklist emerging from stage three (currently in submission), though such efforts would be best led by a consortium of leading companies.

4.2.2 Policy and Guidelines: As noted by the NSPCC, some companies have not been compelled to make changes to their products until threatened with government enforcement. Typically organisations such as FOSI and the NSPCC liaise with government to inform new legislation, but as above, legislation would be better informed by industry being proactive in raising concerns about trends they foresee and new capabilities that may affect risk.

4.2.3 Responsible adults: Organisations such as FOSI and the NSPCC provide materials to educate parents around online safety. Such materials need continual revision to keep apace with technological change, and clearly need updating for the context of IoT. A particular hurdle in creating effective materials of this sort is the complexity and ambiguous nature of IoT which makes it difficult for parents to fully grasp, much less oversee responsibly.

4.2.4 Education: This is the area we are keen to explore in future work. Moving away from our earlier efforts to identify problematic components of the micro:bit and redesigning them for safe use, the next step for our research will be to develop experiential, micro:bit based curricula that confers fundamental lessons in both ethics and online safety that children will need to grasp to capitalize on the technological cornucopia available to them whilst remaining safe. We envisage this taking the form of 'workshops-in-a-box' containing step-by-step build instructions and all the necessary component (sensors, wires, clips), along with detailed lesson plans that educators can use in the classroom to progress children through a series of prompts to provide consideration of salient principles. Adhering to the notion introduced above of 'learning to fall safely', these workshops would allow children to explore risk rather than being risk averse. We believe this approach complements well executed privacy by design, and is highly transferable to new and unpredictable technological contexts, including a future in which IoT is passé and all new digital interactions are on offer. A challenge we anticipate in developing these workshops-in-a-box is the need to customise material for different stages of psychological and moral development, perhaps even starting with children much younger than the 9- to 11-year-olds we worked with in the IoT4Kids project.

5 Conclusion

The interviews and workshop reported in this paper helped highlight the subversive nature of IoT technologies, which increases the likelihood of them being used for abuse. Our key informants stressed the need to develop ways of thinking about IoT risk in a future filled with unknowns. The strategy we used to facilitate productive thought about risks was to engage children in developing sketches of desired uses of the micro:bit, translating those into Use Scenarios, and then seeking expert feedback on the risks posed by these uses of IoT technology. While this approach has its limitations – namely it focused discussions around the BBC micro:bit which is unquestionably the safest IoT device for children – our project partners found the scenarios useful for thinking about risk. Interestingly, our interviews revealed that the process used by the BBC micro:bit developers yielded very similar considerations to those we had identified through our Use Scenarios. This suggests that such a method might be used to formalise the design thinking that goes into developing new IoT devices for children**.**

6 Acknowledgements

This research was supported by the EPSRC through the PETRAS IoT Hub (research grants EP/N023234/1 and EP/N02334X/1) and received ethics approval from Lancaster University (FST17001). We would like to thank our participants for contributing their time and effort.

7 References

[1] NESTA. Next Gen: Transforming the UK into the world's leading talent hub for the video games and visual effects industries, (2013).

https://media.nesta.org.uk/documents/next_gen_wv.pdf, accessed 09/02/2109

[2]The Royal Society. Shutdown or Restart: The way forward for computing education in UK schools. The Royal Academy of Engineering. (2012). https://royalsociety.org/~/media/education/computing-in-schools/2012-01-12-computing-in-schools.pdf, accessed 08/02/2019

[3] Knowles, B., Finney, J, Beck, S and Devine, J. What Children's Imagined Uses of the BBC Micro:bit Tells Us About Designing for their IoT Privacy, Security and Safety. In *Proc. PETRAS Living in the Internet of Things (*2018).

[4] Knowles, B., Beck, S., Finney, J. and Devine, J. Proactively Attending to Potential Risks of IoT for Children. Submitted to Proc. 2019 conference on Designing Interactive Systems (DIS '19). **In submission.**

[5] Georgia M Winters, Leah E Kaylor, and Elizabeth L Jeglic. 2017. Sexual offenders contacting children online: an examination of transcripts of sexual grooming. *Journal of Sexual Aggression, 23*, 1 (2017), 62–76.

[6] BBC News. 2017b. Minecraft paedophile Adam Isaac groomed boys online. http://www.bbc.co.uk/news/ukwales-south-east-wales-38691882.
(2017).

[7] NSPCC (2018) Online Abuse Facts and statistics https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/online-abuse/facts-statistics/ (Accessed 04/08/2108).

[8] Childline (2018) Cyberbullying: Online bullying. https://www.childline.org.uk/info-advice/bullying-abuse-safety/types-bullying/online-bullying/ (Accessed 07/08/2018).

[9] Information Commissioners Office (2018) Guide to the General Data Protection Regulation GDPR- Children: At a glance https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/applications/children/ (Accessed 04/08/2018).

[10] Centre for Information Policy Leadership. (2018). GDPR Implementation
In Respect of Children's Data and Consent. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_gdpr_implementation_in_respect_of_childrens_data_and_consent.pdf (Accessed 07/08/2018).

[11] Frith, E. (2018) Social Media and Children's Mental Health: a review of the evidence. Education Policy Institute https://epi.org.uk/wp-content/uploads/2018/01/Social-Media_Mental-Health_EPI-Report.pdf (Accessed 07/08/2018).

[12] Morris, E. (2016) Children: extremism and online radicalization, Journal of Children and Media, 10:4, 508-514, https://www.tandfonline.com/action/showCitFormats?doi=10.1080%2F17482798.2016.1234736

[13] Roberts J. 2017. Talking Doll CloudPets Leak Kids' Secrets on the Internet.

[14] BBC. German parents told to destroy Cayla dolls over hacking fears. BBC News. 2017 https://www.bbc.co.uk/news/world-europe-39002142 accessed 09/02/2019

.