What Children's Imagined Uses of the BBC micro:bit Tells Us About Designing for their IoT Privacy, Security and Safety

Bran Knowles*, Joe Finney*, Sophie Beck* and James Devine*

** School Of Computing and Communications, Lancaster University, UK*
{b.h.knowles1},{j.finney},{s.beck},{j.devine}@lancaster.ac.uk

Keywords: Internet of Things; Education; BBC micro:bit; Privacy; Security.

Abstract

Ensuring that young people reap the benefits of the Internet of Things requires proactively attending to the risks they may encounter in entering the world this new technology affords. The e-safety guidelines currently taught in UK schools may not sufficiently prepare children for navigating the risks that come with connected devices. In this paper we describe initial results from the PETRAS project IoT4Kids, exploring the privacy and security implications of children programming the BBC micro:bit, an IoT-ready device designed for children. We report on children's (ages 9–10) likely uses of the micro:bit and discuss their implications, highlighting shortcomings of e-safety education and policy guidelines for such uses.

1 Introduction

In June 2017, The Family Online Safety Institute (FOSI) held a roundtable event entitled "Connected Families: The Risks and Opportunities of Connected Devices, Toys and Cars," to foster dialogue on the implications of the changing landscape of children's digital interactions. Readily acknowledged at this event were the novel, exciting benefits (educational and otherwise) that Internet of Things technologies afford for children. On the other hand, leaders in this space—including FOSI as well as, notably, the National Society for the Prevention of Cruelty to Children (NSPCC)—recognise that guidelines and legislation have not kept pace with the technological change represented by the IoT.

The project we report here, known by the acronym IoT4Kids, is a PETRAS IoT Hub project that expands the hub's portfolio to include considerations pertaining specifically to *children's* use of IoT. This project (funded through the PETRAS Partnership Research Fund) involves substantial collaboration with three research partners: The Micro:Bit Educational Foundation, FOSI, and NSPCC. With organisations like FOSI already looking at the various ethical considerations raised by commercially available IoT toys for which there is (at least in theory) some adult oversight of development, IoT4Kids explores what happens when the power to create new and exciting uses of IoT is given to children themselves. While adults may speculate about what children are likely to want to do with this capability, IoT4Kids engages directly with children in envisaging desired uses of programmable IoT—in particular, the BBC micro:bit, developed specifically for young people.

The aim of this paper is to report on the project's initial engagements with participants aged 9–10, elaborating a set of likely micro:bit uses that expose some of the most pressing challenges in designing programmable IoT devices for children. We compare the kinds of challenges such potential uses of the micro:bit expose to the challenges that have been mapped to date in the area of e-safety generally (i.e. web and mobile contexts), and in particular those mapped in relation to IoT toys. We begin by providing background on the landscape of IoT toys and the extent to which current e-safety guidelines lag behind these advances; followed by an introduction to the BBC micro:bit. We then report the results of the participant engagements, and discuss their implications, in particular exploring the potential of the micro:bit as a tool for educating children about the risks associated with IoT that goes beyond and is more experiential than current e-safety curriculum.

2 Background

2.1 IoT Toys

In 2016 the Family Online Safety Institute, published a white paper addressing the concerns around the growing use of 'connected toys' by children. The white paper identifies three categories of toys that utilise emerging technologies [3].

- *Connected Toys* connect to the Internet via Wi-Fi or Bluetooth and collect data from children that is used and stored on the internet. Toys that are connected to the Internet are subject to U.S. privacy laws, i.e. the Children's Online Privacy Protection Act (COPPA).
- *Smart Toys* use computer processing to simulate intelligent interaction with children. The features of such toys could include accelerometers, sensors, compasses, radio transmitters, Bluetooth, cameras, microphones and gyroscopes. Although these toys collect children's data, the privacy concerns are reduced when not connected to the Internet.
- *Connected Smart Toys* can collect personal information from children's play, which combined with Internet connection, enhances the potential for privacy and safety breaches.

To date, the emerging IoT toy market has been notoriously victim to hacking. Privacy and safety breaches of toys such as the My Friend Cayla doll and CloudPets [6] have served to elucidate some of the threats around children's engagements with IoT and highlight the need for engaging in more in-depth conversations around the future ethical implications of such technologies. Thus far the toy industry has been left to self-regulate on matters regarding child privacy and safety, with larger toy companies (e.g. those producing Cognitoys Dino and Hello Barbie) leading the way on best practice in security design for toys [8]. But given the vulnerabilities of target users of such technology (i.e. children), it is essential that "children, regulators, law enforcement, and educators" [5] take part in shaping our understanding of the risks and benefits of new technologies towards the development of e-safety legislation reflective of the new technological landscape of the IoT.

2.2 Policy Guidance and e-Safety in Schools

As ICT is now integral to children's everyday lives—at home, socially and in the school setting—e-safety requirements have evolved to cater for the emerging risks children face when using ICT. Schools play a key role in delivering e-safety curriculum, with the Department for Education's (DfE) "Keeping Children Safe in Education" providing the latest statuary requirements for schools [2]. Ofsted also provides guidance for inspectors to measure schools on their incorporation of e-safety guidelines into their curricula [6]. As technologies have changed, the remit of e-safety statuary requirements for schools has expanded to include issues relating to the use of social media and mobile technology, now covering bullying, radicalisation, child sexual exploitation and trafficking, and sexting, among others.

The NSPCC offer materials to support schools, parents and children in raising awareness and education on e-safety. The latest materials offer guidance pertaining to "websites, email, instant messaging, chat rooms, social media, mobile phones, blogs, podcasts, downloads, virtual learning platforms" [9], but these need updating for the new contexts created by IoT toys and programmable IOT.

2.3 The micro:bit as a Programmable IoT Device

In order to contribute toward the development of guidelines and legislation that respond adequately to the emergent privacy, security and safety threats associated with IoT devices, the IoT4Kids project explores potential uses of an IoT platform that has been designed to be programmable by children—namely the BBC micro:bit. Powered by an ARM microcontroller, the BBC micro:bit (Figure 1) has an onboard 5x5 LED array, buttons, accelerometer, compass, temperature and light sensors, Bluetooth radio, and an edge connector for touch sense and expansion. It may be connected to USB or Bluetooth for programming, and it can be powered by USB or battery. Creating programs for the device is simple and requires no software installation. Programs can be written in Blocks (a visual programming language), JavaScript, and Python. Programs are transferred to the device using a simple drag-and-drop file transfer to the micro:bit, which appears as a USB mass storage device.

The original motivation of the consortium of industry and academic partners who developed the micro:bit (organised and overseen by The Micro:Bit Educational Foundation, an IoT4Kids project partner) was to inspire children to learn the principles of computer science and engineering through engaging creatively with the micro:bit to explore a world where sensor-based devices are ubiquitous. Careful consideration was given to the visual design of the device, adding elements to present a friendly face to engage those who consider themselves less technical. Care was taken to separate the user interaction ('fun') side of the board from the components that made user interaction possible. No attempt was made to hide the more technical components. Quite the opposite: they were clearly labelled and explained as an invitation to explore and engage with their purpose.

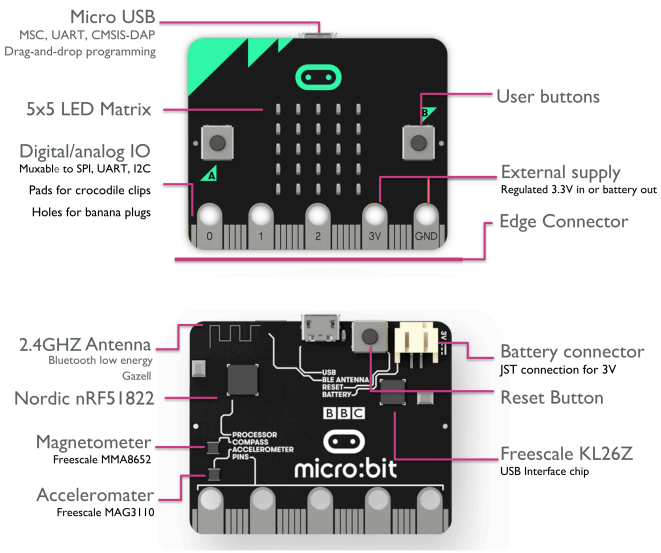

Figure 1: The BBC micro:bit.

The BBC micro:bit debuted in the 2015-2016 school year in the UK, when micro:bits were distributed for free to Year 7 (11-12 year old) students and their teachers. Over 750,000 devices have been delivered into schools, providing 90% coverage of all UK mainstream high schools. Critically for our research interests, although the micro:bit was always designed with the intention of being a programmable IoT device[1], developers took a very considered ethical approach to developing their device—purposefully restricting some functions, like those involved with radio communication, and strengthening security around others, such as Bluetooth

[1] Other programmable IoT devices include Arduino and Raspberry Pi, both of which have seen some adoption in the classroom. Unlike the micro:bit, however, both of these ecosystems presume a basic level of proficiency: knowledge of electronics and circuitry, the ability to program, the ability to configure networks, the ability to configure and install software—traits not commonly seen in children.

pairing, due to concerns around safety and privacy of child users. As such, while of great interest to The Micro:Bit Educational Foundation, true IoT scenarios have not yet been realised through micro:bit related curricula.

3 Outreach Day 1 and Results

The IoT4Kids project will comprise Outreach Days with a total of 55+ students from local schools ages 9–12. The aim of these events is to elicit desired uses of programmable IoT in order to identify privacy and security risks associated with such uses; and then to inform the development of curriculum (hands-on micro:bit activities) and new policy guidelines surrounding children's engagements with IoT.

We report below the results from our first Outreach Day, with 32 children ages 9–10. At the start of the day, project researchers presented some example uses of the micro:bit by way of background to the tool; then children were given a hands-on task that introduced them to the basics of how to programme it. Afterwards, children were asked to write down as many ideas as they could think of for what they wanted to use the micro:bit to do; and then to choose one of these ideas to expand further using a worksheet with space for sketches. Researchers recorded discussions they had with children as they developed their ideas, and further quotes were captured when a number of children chose to take part in one-minute presentations of their ideas.

Following the event, we conducted a clustering exercise to identify similarities in desired uses of the micro:bit. We have selected four to describe in detail below. While these do not represent the full range of use scenarios emerging from the data, we focus on these due to the interesting and varied concerns they elicit. We present these categories of use below in (approximate) ascending order of risk.

3.1 Assistance

Several children imagined uses of the micro:bit as a technology that could help them with mundane tasks. Your Robot Helper, for example, reminds the child when to perform activities (such as eating), and provides weather reports to help him plan his day. Or the micro:bit could be programmed to work as a universal remote control for laptops, tablets, phones and toys (Figure 2a), and in addition, "If you lose the remote it will take over." The voice-activated Micro:Voice (Figure 2b) tracks a child's location to tell him where he is and direct him if he gets lost; and "If you forgot your phone, you can ask it stuff, call people and many other things."

In contrast to some of the use scenarios we report below, these concepts are easily implementable using the components available with the micro:bit. Unconnected, these assistance technologies pose very little risk (as identified by COPPA (see [3])), and building such tools could make for fun learning activities—precisely the kinds of tools the micro:bit was designed to help children program. The micro:bit does not have inbuilt tracking facilities. Once connected, however, designs that utilise GPS and/or the micro:bit's accelerometer to collect data that reveals movement through a space or a child's daily routines could present risks of predatory stalking. Notably, a high number of participant designs required that the device capture one or more high-risk categories of data—including photographs, video, or audio containing the child's image, or voice; or geo-location—that have been shown in the case of IoT toys to put children at risk (see [3, 11]).

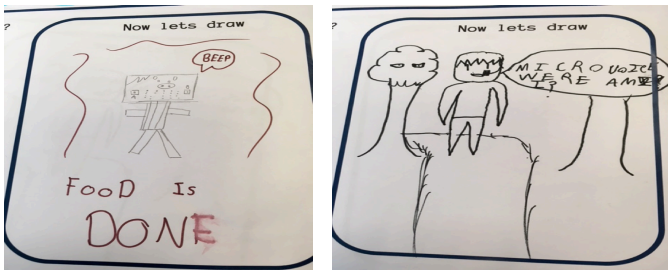

Figure 2: (a) Your Robot Helper; (b) Micro:Voice

There are, however, participant designs that introduce further problematic elements to these assistive technologies. For example, The Micro:kid Detector monitors a child's behaviour, taking the kind of tracking seen in the examples above to the level of surveillance: "This will help you by not getting your child in trouble and also by stopping them. When they are going to do something bad it will make a buzzing sound." The micro:bit includes a motion sensor which could be instrumentalised around key objects (e.g. a cookie jar) for this kind of purpose; and the micro:bit could also be linked to other technologies such as cameras or voice recognition to provide further surveillance. While the ability to predict intent for bad behaviour with any sort of precision is beyond the sensing capabilities of the micro:bit, studies have demonstrated how people are capable of gleaning a great deal of information from family members' activities from seemingly innocuous data [13]. IoT toys have raised new questions around a child's right to privacy from his/her own family members [7]; but given that children may wish to develop tools that capture some details about their activities, important considerations are how doing so may affect the parent-child relationship and infringe on a child's right to privacy, and whether children have sufficient understanding of these dynamics to be able to make responsible programming decisions.

3.2 Education

Different to the above, children envisaged potential for the micro:bit to connect them to information, and to take part in a two-way sharing of this information. The micro:bit was indeed seen as a way to "replace teachers across the world" with more individualised tutoring: "Instead, there will be robots to teach every single child" (The Micro:bit Teacher). A slightly different take on this theme was the similarly named Robotic Teacher 2000 (Figure 3a), that used the micro:bit to enable children "to talk to other children and robots."

Effectively a peer-to-peer network, this tool would ostensibly connect a group of learners who might then engage in productive exchange of information; meanwhile the tool could monitor each individual child's learning progression.

The micro:bit has the potential for educational purposes and has already seen uses in classroom settings. Examples of quizzing students using the yes/no buttons provide exciting possibilities for making learning fun. The risks change, however, when that education is realised through connected devices. Notably, both of these examples seek to replace a teacher with a robot, and in doing so relocate the trust that a child might reasonably hold in a teacher onto a device. That assumed trust is easily preyed upon if a device is hacked. While not specifically mentioned as part of the design, it is potentially within reach for rudimentary implementations of such concepts to record the child's dialogue (with the device and/or peers) for ease of review of the information exchanged. Here, concerns that were raised around the hackability of tools like Siri and Alexa are clearly relevant, namely that personal information might be stolen if hacked [1].

3.3 Play

Another desired use of the micro:bit was to enable simulation of activities children are not normally able to engage in. The Micro:bit Car (Figure 3b), for example, would allow a child to take over and drive an adult car. Rather than using the physical controls in the car, a pre-programmed device would allow them to drive it as a game simulator. Adding further elements of simulation, The Micro:bit Car VR is a virtual reality headset that provides the child with an opportunity to play out imagined, scary experiences, such as a zombie apocalypse, war with intergalactic beings and world take over, hostage capture, and driving through hostile environments.

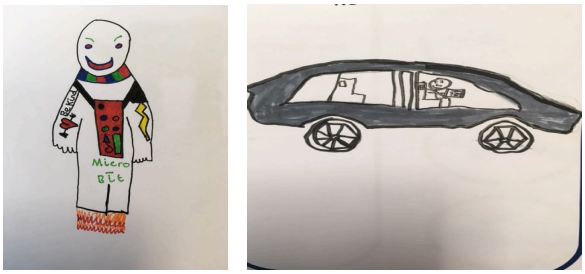

Figure 3: (a) Robotic Teacher 2000; (b) The micro:bit Car

Importantly, these examples illustrate young people's—in these particular cases, boys'—desire to "pla[y] at being a part of the risky adult world" [14], experiencing dangerous scenarios as a way of experimenting with these risks. Children engaging in such activity fall into the victim category of "Risk Takers" [14], i.e. displaying disinhibited behaviours and seeking adventure. Online groomers have been known to capitalise on risk-taking behaviour, using gaming platforms in particular as a means of contacting and ultimately grooming young boys [14].

It is entirely feasible that the micro:bit could be programmed to move an object in another location. What object is moved, where it is moved to, and what the intentions and perceptions of that activity are will be what determine the degree of risk posed by this capability in specific contexts. As an illustrative if over-the-top example, a child seeking to elicit fear in others might use the micro:bit to move a wheelchair with a chainsaw attached to it into a room full of people. Less dramatically, a child might use a micro:bit controlled car to shoplift or steal sweets from their peers. Given the range of activities that might be enabled by remote control of objects, it is important that education around engagements with the IoT include emphasising that the same rules of 'good' and 'bad' behaviour apply even (or perhaps particularly) when the child doing the behaviour is not easily visible or identifiable to others. This means helping reinforce the internalisation of morality, rather than teaching children that something is 'bad' because they will get in trouble for it.

3.4 Companionship

A number of participants—interestingly, overwhelmingly girls—described uses of the micro:bit for assuaging loneliness. For example, Figure 4a is a sketch of a friendless child, alone in her room, for whom the micro:bit offers the opportunity of virtual friendship. The creator of this design explained that "you can program it to be your friend if you don't have any…and make it talk to you so you are not lonely." Along these same lines, Starburst (Figure 4b) is a soft and cuddly trusted companion, programmed to offer affection and play the part of a personal best friend: "When you are sad it cuddles you, when you had an argument with your friend it cheers you up, it solves your problems, it teaches you things you don't know, it tells you bedtime stories (if you want it to). It is your dream." Here the micro:bit is seen as a means of compensating for a lack of affection, at times of great sadness, as is also the case in the Hug Monitor (Figure 4c): "when you're down in the dumps," this teddy will recognise your emotions and hug you.

Using a connected device as a tool for emotional support, nurturing and companionship entails the device somehow monitoring negative emotions and detecting moments of peak vulnerability—perhaps best illustrated by the Cop Caller (Figure 4d), which recognises when a child is in danger and calls the police. Critically, a child who creates an emotional, trusting bond with a digital 'thing', capable of mimicking human interaction and affection, is at greater risk of becoming a victim of online grooming, (ironically) bullying, and radicalisation. Online crime of this sort tends to feed on vulnerable children, particularly those with low self-esteem or those facing adversity [14]. Predators are known to adapt their digital personas in order to more effectively engage with children, for example acting as a "mentor" [14]. Assuming one of the above designs were hacked, a predator might engage directly with children in their personal space, commandeering the personalities of the toys in ways the child is unable to detect.

Figure 4: (a) My Plans for People with No Friends; (b) Unicorn Robot Teddy, Starburst; (c) Hug Monitor; (d) Robot Racing Car 90000! Cop Caller

Elements of these designs are already commercially available in IoT toys, but it is worth noting that companionship can be realised in a rudimentary manner through tools like the micro:bit that children may program themselves. For example, a child could program buttons to enable them to indicate if they are happy or sad (pressing A or B), and then beacon out this information in ways that can be intercepted, i.e. via pair programming. A predator—or slightly less sinister, a bully—would then be able to send the child messages of comfort using the LED screen, cultivating the child's trust before leading on to more intimidating or coercive communication. The apparent desire of children to reach out for comfort at times of vulnerability indicates the importance of educating around detecting when a device has been hacked (or paired) by a predator, and how to ensure that device communication is secure.

4 Discussion

IoT devices are potentially changing the way that children play and interact with everyday objects [1, 7]. Current guidance for IoT is aimed at parents and educators, and yet many parents and teachers lack of awareness of the risks associated with IoT [4, 7, 8]. While it is the parent who typically makes device purchasing decisions on behalf of their child, the adaptability of programmable IoT platforms makes it difficult for parents to anticipate how their child may ultimately engage with the IoT. This suggests that children are going to have to assume greater responsibility for ensuring their own privacy, security and safety. As the participant examples above indicate, in addition to e-safety curriculum currently delivered in schools around predatory behaviour, radicalisation, bullying and sexting, children will need to be equipped with basic literacy around ethical concepts such as privacy and consent, and technical concepts such as how data is produced and used by devices they engage with and how they may be hacked or hijacked. Larger discussions also need to be facilitated with legislators and the public around ethical matters such as the degree of privacy children ought to have as a right, and how, if they are to have greater responsibility for their own personal data, informed consent might be achieved for child data creators.

Given the ever changing natures of technology and the capabilities of predators and malevolent agents, perhaps more so than learning specific strategies for keeping personal data secure, children need to develop critical thinking in their interactions with technologies such as IoT [10]. Future devices in this space will almost certainly include built-in Wifi, making it easier for children to both intentionally and unintentionally transmit personal information. In contrast, having been built through a 'privacy by design' approach, the micro:bit may offer a unique learning experience whereby children can develop critical thinking skills through exploring the capabilities of an IoT device within a secure learning environment before they are likely to engage with the marketplace of less cautiously designed IoT devices. Just as the micro:bit has been utilised in playful approaches to 'snoop on signals', e.g. collecting data from a wireless keyboard [12], a playful approach could be useful for exploring data breaches and hacking, as well as where the safety threshold lies on data capture, moving from non-threatening data such as step counter to when a movement monitor connects to the Internet and collects personal data for health analytics. For example, educational activities could be developed that get peers to act as detectives, trying to find out whatever information they can from the user as they step through these different kinds of data.

5 Future Work

IoT4Kids is very much in its early stages. Additional Outreach Days with slightly older children (ages 11–12), currently in preparation, may elicit further desired uses of the micro:bit that present risks to children. Once the data collection from these engagements is completed, the next step for the project is to develop 'use scenarios' that more fully elaborate the ways in which the micro:bit, or indeed other similar devices, might be appropriated to meet aims such as those described above (assistance, education, play, companionship). These use scenarios will take the form of amalgamated and fictionalised (narrative) versions of the designs produced by project participants, and will include greater details of the kinds of sensors and other devices children may attach to the micro:bit to approximate their fantastical design ambitions. Next, these use scenarios will be used to prompt discussion with key informant interviewees from partner organisations: FOSI, NSPCC and The Micro:bit Educational Foundation consortium. Interviews will seek to elicit expert opinions regarding the real-world risks posed by such uses, generate amendments to existing guidance aimed at parents and educators, and explore the development of curricula that may better educate children about how to safely engage with IoT. At present, we offer this paper as our initial musings regarding the salient privacy, security and safety considerations surrounding programmable IoT for children.

6 Conclusion

In this paper we identified four types of uses of the micro:bit that children claim they want. These should not be viewed as a comprehensive set; rather, we hope that they shed light on some of the risks children may face when attempting to harness IoT technologies. While there are obvious ways to restrict children's use of the micro:bit so that these risks are minimised or even eliminated, we see greater sense in aiming to educate parents and educators (through new guidelines), but most importantly children themselves (through experiential learning activities), about how they may interact safely with the full range of IoT technologies they could encounter.

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 Lancaster University's Computing At Schools (CAS) programme for helping us organise and facilitate the participant Outreach Days, with special thanks to Geraint Harries and Lorraine Underwood. We also thank the teachers and students who took part in the study.

References

[1] M. Courtney. 2017. Alexa, Cortana, Siri et al: do our digital assistants hear more than we want them to? *E&T Magazine.* https://eandt.theiet.org/content/articles/2017/10/alexa-cortana-siri-et-al-do-our-digital-assistants-hear-more-than-we-want-them-to/. (2017). (Accessed on 01/09/2018).

[2] Department for Education. 2016. Keeping children Safe In Education: Statutory guidance for schools and colleges. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/550511/Keeping_children_safe_in_education.pdf. (2016). (Accessed on 01/09/2018).

[3] Family Online Safety Institute. 2016. Kids & The Connected Home: Privacy in the Age of Connected Dolls, Talking Dinosaurs, and Battling Robots. https://fpf.org/wp-content/uploads/2016/11/Kids-The-Connected-Home-Privacy-in-the-Age-of-Connected-Dolls-Talking-Dinosaurs-and-Battling-Robots.pdf.

[4] Family Online Safety Institute. 2016. Connected Families: How Parents Think & Feel about Wearables, Toys, and the Internet of Things. https://www.fosi.org/policy-research/connected-families/. (2016). (Accessed on 01/09/2018).

[5] Family Online Safety Institute. 2017. FOSI Roundtable: Connected Families. The risks and opportunities of connected devices, Toys and Cars. https://www.fosi.org/events/fosi-roundtable-connected-families/. (2017). (Accessed on 01/09/2018).

[6] Roberts J. 2017. Talking Doll CloudPets Leak Kids' Secrets on the Internet. http://fortune.com/2017/02/28/cloudpets-data-leak/. (2017). (Accessed on 01/09/2018).

[7] Andrew Manches, Pauline Duncan, Lydia Plowman, and Shari Sabeti. 2015. Three questions about the Internet of things and children. *TechTrends 59,* 1 (2015), 76.

[8] Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. 2017. Toys that Listen: A Study of Parents, Children, and Internet-Connected Toys. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems.* ACM, 5197–5207.

[9] NSPCC. 2017. E-safety for schools. https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/e-safety-schools/. (2017). (Accessed on 01/09/2018).

[10] NSPCC. 2017. Technology, toys and the internet. https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/technology-toys-and-the-internet/. (2017). (Accessed on 01/09/2018).

[11] Federal Bureau of Investigation. 2017. Internet-Connected Toys Could Present Privacy and Contact Concerns for Children. https://www.ic3.gov/media/2017/170717.aspx. (2017). (Accessed on 01/09/2018).

[12] I Thomson. 2017. BBC's Micro:bit turns out to be an excellent drone hijacking tool. https://www.theregister.co.uk/2017/07/29/bbcs_microbit_drone_hijacking_tool/. (2017). (Accessed on 01/02/2018).

[13] Peter Tolmie, Andy Crabtree, Tom Rodden, James Colley, and Ewa Luger. 2016. "This has to be the cats": Personal Data Legibility in Networked Sensing Systems. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing.* ACM, 491–502.

[14] Stephen Webster, Julia Davidson, Antonia Bifulco, Petter Gottschalk, Vincenzo Caretti, Thierry Pham, Julie Grove-Hills, Caroline Turley, Charlotte Tompkins, Stefano Ciulla, et al. 2012. European online grooming project (Final report). *European Commission Safer Internet Plus Programme, Tech. Rep.* (2012).