A Scenario-Based Methodology for Exploring Risks: Children and Programmable IoT

Bran Knowles, Sophie Beck, Joe Finney, James Devine, Joseph Lindley
Lancaster University
Lancaster, UK
[b.h.knowles1, s.beck, j.finney, j.devine, j.lindley]@lancaster.ac.uk

ABSTRACT

In this paper we report on research exploring the privacy, security and safety implications of children being able to program Internet of Things devices. We present our methodology for understanding the contexts in which children may wish to use programmable IoT, identifying risks that emerge in such contexts, and creating a set of questions that might guide design of such technologies so that they are safe for child users. We evaluate the success of the methodology, discuss the limitations of the approach, and describe future work.

Author Keywords

Children; Internet of Things; IoT; ethics; privacy; micro:bit; participatory design

INTRODUCTION

With the Internet of Things (IoT), new forms of technological engagements are possible not only for adults but also for children. As the IoT vision takes tangible shape, concerns regarding privacy, security, and reliability have emerged, alongside various ethical concerns. Concerns pertaining to children and IoT have thus far centred around their use of connected smart toys [16, 17], neglecting the potential for children to appropriate programmable IoT Maker platforms, or indeed use platforms that are designed specifically for child programmers, to access a world of risks that they may be ill-prepared to navigate. Particularly concerning is that children who may still have critical gaps in their privacy and security understandings are being enabled to program IoT devices, and that parents' own lack of technical understanding of IoT may make it difficult for them to provide assistance to their children in managing their privacy and security concerns as they do with other digital technologies [12].

Children programming IoT is not the distant possibility it may seem. Physical computing is being introduced into classrooms as an alternative to screen-based computing education [27], and this approach has been shown to have certain advantages in terms of promoting motivation, collaboration, creativity and tangibility [28]. In particular, the BBC micro:bit (see http://microbit.org/) has been developed as a platform for teaching children the principles of computer science and engineering by engaging them in creative play in the sensor-based world that surrounds them. A child-friendly design makes it possible for children to learn to create basic devices in under an hour and progress to more advanced IoT device creations through experimentation with the many different components, including connectors for attaching external sensors. In contrast to other programmable IoT devices (e.g. Arduino and Raspberry Pi) that have seen some adoption in the classroom, the micro:bit ecosystem does not presume a level of proficiency that includes knowledge of electronics and circuitry and the ability to program, configure networks, or configure and install software. Careful consideration was given to the visual design elements of the device so that it would engage truly novice, and possibly timid, technologists; programming was made accessible through a visual programming language and drag-and-drop file transfer to the micro:bit; all of which was underpinned by a constructionist [23] approach that promotes learning of computer programming—including sequential progression through more advanced languages such as JavaScript and Python—through creative experimentation in a world where sensor-based devices are ubiquitous.

Having developed a tool that enabled children to program the Internet of Things, the makers of the BBC micro:bit were concerned about the privacy, security and safety implications of deploying the device; hence, a decision was made to restrict some functions like those involved with radio communication, strengthen security around others such as Bluetooth pairing, and limit its use to safe educational (closed) environments. In this state, there are few if any risks to children, but this is traded off against the learning potential of the device. According to one of the BBC micro:bit's developers, "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" (key informant interviewee). 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

DIS '19, June 23–28, 2019, San Diego, CA, USA

DOI: https://doi.org/10.1145/3322276.3322315

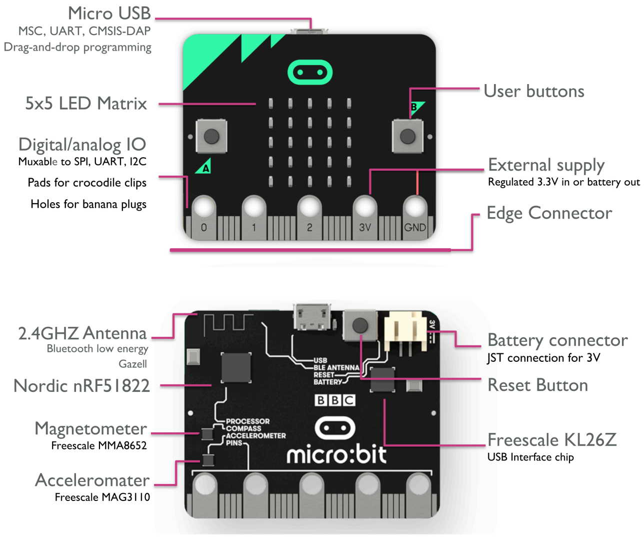

Figure 1. The BBC micro:bit.

which will not have been designed with such a clear ethical imperative and focus on vulnerabilities of child users.

In the UK, efforts at formal training around online safety has evolved from static webpage interaction advice to include guidance surrounding Web 2.0 and mobile interactions, covering new territory such as social media bullying and sexting; but as yet there is no IoT component to this curriculum. Some guidance has been developed by organizations such as the Family Online Safety Institute (FOSI) and the National Society for the Prevention of Cruelty to Children (NSPCC) to support parents and children in navigating emergent risks in the marketplace of smart connected toys,[1] but this guidance pertains to interactions that are developed by adults and governed by increasingly strict privacy and security legislation as enforced by the Children's Online Privacy Protection Act (COPPA) in the US and the new European General Data Protection Regulation (GDPR). As digitally adept children find new ways to capitalize on the creative control afforded by readily available and increasingly diverse platforms for developing their own IoT devices, designers will need new strategies for anticipating the risks presented by their technologies across the full potential of contexts in which they may be used by children, as well as new tools for evaluating whether they have attended to all relevant considerations in these contexts.

In this paper we present and evaluate a novel methodology for envisaging risks and identifying pertinent questions that might guide the design process toward ethically sound technology outputs. We demonstrate this methodology in action in IoT4Kids, a study exploring what children are likely to do with their new capabilities to create their own IoT device interactions, and what risks they are likely to encounter as a result. We identify three key categories of desired use that have emerged through workshops with child participants and illustrate potential risks of such uses through "use scenarios", i.e. fictional amalgamations of participants' own designs. These are then used as the basis for developing a Risk Mitigation Checklist. Drawing from the use scenarios, the checklist contains salient design considerations that might underpin a privacy by design approach when developing IoT for children. We end by evaluating the success of the methodology, discussing the limitations of the approach, and describing future work.

INTERNET OF THINGS CONTEXT

A relevant backdrop to this work is the uniqueness of IoT devices, principally that they exhibit agendas and agency which are entirely unrelated to elements of the design the user sees and interacts with. In these contexts, it cannot be assumed that any given device, software, or service is solely designed to help the user achieve a headline activity. As an example, the manufacturer Vizio sold smart televisions that logged the programs users were watching and passed this information to third parties for the purpose of marketing. Vizio became notorious because the company failed to include details of this activity in the device's user agreement, hence the data gathering task was illegal. The data that was logged and passed to third parties had absolutely no relevance to the user's activity (watching television).

What further differentiates IoT devices from their non-IoT counterparts is not simply the complexity which occurs in systems, but rather the new types of agency, value, and power that they enable through the "networkification of the existing non-Internet world" [25]. IoT devices often have a digital shadow (i.e. data), which, although usually resulting directly from an interaction, is rarely visible at the time that action takes place. These data are essential to making the things of the IoT work. For example, data may feed learning algorithms; may be central to a company's business model; may be necessary to drive a device's functionality; or could be necessary to fulfill a regulatory requirement. In some circumstances these present-but-unseen data mean that significant portions of an IoT device's agency may be obscured, undermining the agency of the human user.

These properties present a significant design challenge in terms of protecting users from malevolent actors and enabling informed consent, in particular when it comes to vulnerable child users. Critically, IoT affords a multiplicity of potential devices and use contexts on a scale not normally encountered by designers, for which risks emerge throughout a constellation of connected devices and services. We argue that new methodologies are needed for expanding thinking to risks not readily apparent to developers of IoT devices; and while the methodology we present in this paper is not the definitive answer to this, it does open up an avenue for future work that may prove helpful.

APPROACH AND FINDINGS

The aim of our project, IoT4Kids, was to understand the potential uses of programmable IoT by children so that we might anticipate the privacy, security and safety risks that emerge in

[1] This is an active area of work for FOSI, as evidenced by their policy research [6], round table events [8] and white papers [7]; and is a more nascent area of interest for NSPCC [22].

the context of such uses. An overview of our methodology is as follows:

- *Student Engagement Days*: To elicit programmable IoT uses, we invited children who were old enough to grasp a visual programming language (Blocks) to learn how to program the BBC micro:bit, see inspirational examples of what other children have used the micro:bit to create, and then to complete an activity to design (sketch) their own micro:bit creation.

- *Team and Partner Workshops*: To better understand the privacy, security and safety implications of the children's design ideas, we explored as a team the technical feasibility of these ideas, i.e. how a child might realistically satisfy the motivation underpinning their design using components that would be available to them. We then conducted two Partner Workshops with project partners FOSI and the NSPCC to understand how these real world uses of the micro:bit might map onto known risks relating to predatory behavior.

- *Use Scenarios*: To communicate our findings of the risks of children programming the BBC micro:bit and similar devices, we translated our insights into amalgamated, persona-based 'use scenarios.' We elicited further feedback on the implications of the use scenarios from key informants at The Micro:bit Educational Foundation, FOSI and NSPCC.

- *Guiding Questions*: To develop guidelines for the development of acceptable programmable IoT devices for children, we extracted key questions emerging from our use scenarios that would focus design thinking toward relevant risks, thereby enabling developers to proactively attend to these risks at design time.

We provide further detail on these stages of research below.

STUDENT ENGAGEMENT DAYS

We ran two engagement days, recruiting a class of 32 Year 5 students (ages 9-10) and a class of 25 Year 6 students (ages 10-11). Three adults—teachers and teaching assistants—were present at each event to provide familiar authority to assist the researchers in managing the children, and to ensure children were supervised throughout the day; they did not lead any portion of the instruction or design activity. The focus for the first half of the engagement days was to deliver a unique educational experience (university outreach) to local schools, aiming to ensure that the children directly benefited from their participation. The second half was oriented toward data collection, with a secondary aim of inspiring children to take an interest in computer science. This was framed as an imaginative design task guided by the question, "What would you love to build with your micro:bit?" In designing the activities, we drew from [5] to maximize the children's role as informants. Recognizing that technology-based imaginative tasks can be difficult for children [9], we scaffolded (see [18]) the task with activity sheets that provided gentle prompts. Students were asked to complete two such sheets (Figures 3 and 4):

1. Working in small groups (5-6 students, 15 minutes), they wrote their exciting ideas into thought bubbles;

Figure 2. Activity to teach children how to program the micro:bit.

2. Working independently (30 minutes), they developed their favorite idea further, giving their concept a title and a description, writing who it was for, and drawing their design.

Our methods emulate the drawing-telling technique created by [34] and used by [4]. Researchers walked around throughout the creative activities, speaking to children about what they were drawing and recording these conversations to be later transcribed. In the first engagement day (with the 9–10-year-olds) but not the second (with the 10–11-year-olds), there was time for children to do a one-minute presentation of their idea, with about 75% eagerly volunteering to present. These presentations were also audio recorded and transcribed. Our final dataset contained transcripts of conversations with and presentations by children about their designs, and design artifacts (completed worksheets).

The research team then carried out a clustering activity on the design artifacts (drawing on information provided about them in conversation with the children) using an iterative inductive coding approach to develop broad categories of use. We began by identifying groupings of designs that bore a similarity with one another, and provisionally named that similarity. In refining our proto-categories, we sought to identify categories that described the same order of thing, arriving at categories that described "what the child wants from the tool." Our coding and analysis was further supplemented by desk research. To account for uses that might not have emerged in our engagement days (either by chance or as a function of our particular workshop design), project researchers looked at the kinds of devices other children have developed using the micro:bit, looking at online posts as well as records kept by project partners the Micro:bit Educational Foundation. We continued coding these uses until the researchers reached saturation, i.e. no new categories were found. In total, we identified three distinct categories as described below.

Assistance

Designs in this category were often motivated by a desire to complete mundane tasks, perhaps in a more effective or at least more interesting way. These tools included simple reminder/alarm devices, activity trackers, universal remote controls, trackers for lost items, and navigation/direction. However, they also included surveillance-based concepts, for example: "When they are doing something bad it will make a buzzing sound;" "[I]f your kids are in their bedroom playing the micro:bit can tell you [the parent] if they are doing anything wrong;" and "[I]f you are still in bed, even if you stand

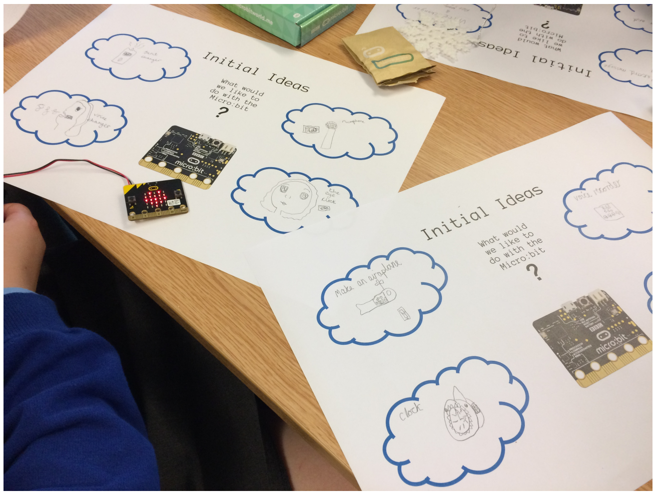
Initial Ideas
What would we like to do with the Micro:bit
?
Initial Ideas
What would we like to do with the Micro:bit
?
micro:bit
Make an aeroplane
Clock

Figure 3. Worksheet exercises part 1.

up to turn [off your alarm clock] and get back into bed, it will still know." A significant majority of designs, both by our own participants and by other children creating with the micro:bit, fell into this category.

Common characteristics of this type included: a) activity and/or location tracking, e.g. made possible by linking in with externally managed systems and databases; b) building a profile of one's activities through time and space; and c) placing trust in the guidance provided by the device.

Play

These designs were motivated by a desire to experience simulation of activities that children are otherwise unable to experience or forbidden from engaging in. Children imagined using the micro:bit to take over and drive a car; providing a point of access to virtual simulation of a zombie apocalypse; or controlling lights and sounds to create a haunted house effect to scare siblings. The focus of this category is on 'risky play' (including 'pranking') as meaningfully distinguishable from 'intimate play' (see Companionship below).

Common characteristics of this type included: a) fulfilment of risk taking behavior; b) meting out punishment or enacting retribution, and c) leveraging technology to distance oneself from or cloak a 'crime', e.g. doing something that is socially inappropriate for which the child would otherwise face punishment.

Companionship

These designs were motivated by a desire for emotional support and the easing of loneliness. Designs often incorporated the micro:bit into toys or dolls to make them more interactive. As children described, "[Y]ou can program it to be your friend if you don't have any... and make it talk to you so you are not lonely;" or similarly, "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." A slight variation on this theme was the idea of being able to send out a distress call to a rescuer, with the device communicating, "I don't like being on my own with no friends, please help me."

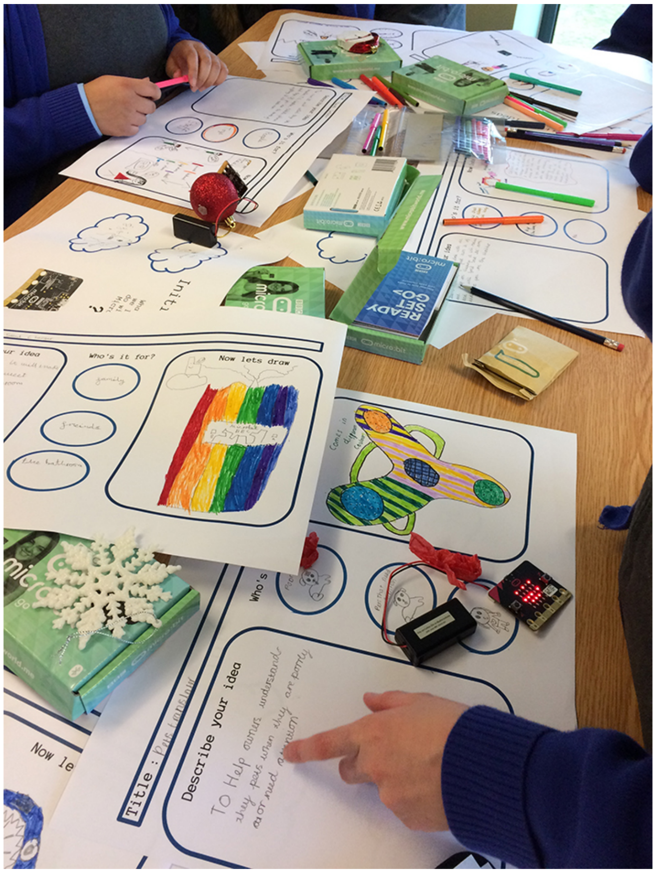

Figure 4. Worksheet exercises part 2.

Common characteristics of this type included: a) monitoring of negative emotions, e.g. fear and sadness; b) mimicking human interaction, e.g. affection, friendship, love; and c) providing a source of nurture.

TEAM AND PARTNER WORKSHOPS

Insights gleaned from the student engagement days were shared among the project team and with project partners. Team Workshops explored how the children's desired uses of the micro:bit might be realized (or approximated) by children with basic to moderately advanced programming skills using readily available technical components. This resulted in several prototypical design concepts that amalgamated children's real and desired uses of the micro:bit, and initial story concepts (including personas and motivations) for plausible real world use scenarios. Partner Workshops were then conducted with representatives from FOSI and the NSPCC to identify the types of risks the children's uses might expose them to. Researchers presented the prototypes and their backstories to the partners, and proposed risks that were evident from our technical perspective. Partners then offered feedback and assisted in further identification and elaboration of risks from their perspectives as experts in predatory behavior.

USE SCENARIOS

Drawing from our understanding of desired uses of the micro:bit, plausible routes by which children might technically realize these desires, the risks they introduce with various design decisions, and contexts of vulnerability that may affect how the child interacts with their device, we more fully developed our set of prototypes and personas and wove them into fictionalized use scenarios. This exercise enabled us to explore how different ways a child might satisfy a particular design motivation affects the kinds of risks they are ultimately exposed to. We discussed our findings with key informants at The Micro:bit Educational Foundation[2] to garner feedback on the key takeaways from our use scenarios and to gain an understanding of how our process for identifying risks compared with their own processes. We further conferred with our partners at the NSPCC to understand how risks to children in other online environments might map to our use scenarios and iterated them accordingly.

For this paper, we present only three use scenarios: one from each use category which together reflect the spectrum of privacy, security and safety implications of children programming IoT devices. Each scenario is presented in three parts: 1) a fictional narrative describing a child's use of the micro:bit; 2) an analysis of the risks entailed by that use; and 3) a discussion of other risks pertinent to the use category (Assistance, Play, and Companionship, respectively).

Maia

Maia is eleven years old and lives at home with her parents and younger sister. Her parents work long hours, so with much to do in the evenings they are very strict with the kids' bedtime, ensuring they are settled down with lights out earlier than most other children in her class. She shares a bedroom with her sister, and on occasion they will get giggly at bedtime, which Mum discourages by restricting their treats.

One night while the sisters lay awake in bed, Maia whispers, "I can't sleep. It's too early to go to bed." Her sister agrees, and they come up with a plan: they will be quiet and pretend to be asleep until they know their parents have gone to bed, and then get up for a tea party and a play. But they discover it is hard to know for sure when their parents are asleep, and they don't want to get caught.

Maia has recently learned how to use a micro:bit, and it occurs to her that she could use it to alert her when her parents are in their bed. She connects her micro:bit to a force sensing resistor and programs the LED array to light up when it senses pressure. After several successful trials in their own beds, Maia sneaks into their bedroom and places the sensor under her parents' mattress while her sister is distracting them. That night, they wait for the micro:bit to light up, and to make sure their parents are asleep, they wait 30 minutes before sneaking downstairs for their first Midnight Feast.

Risks to Maia (and her parents)

The risks that are normally identified relating to IoT are those that are directly mediated by data, i.e. what we might call 'digital risks.' But Maia demonstrates that risks occur in the physical realm too, as a direct result of engagements with IoT platforms. In her case, Maia is using the micro:bit to arrange a situation where she can act without adult supervision, in direct contravention of the rules laid down by her parents. There are real world examples where doing so has resulted in serious harm. In 2017, for example, several young girls incurred serious burns as a result of the social media game Fire Fairy [30]. The game, which lured young girls who were fans of the television show "Winx Club: School of Witches," instructed them:

> "At midnight when everybody is asleep, get up from your bed and go around the room three times, then say the magical words: 'Alfey kingdom, sweet little fairies, give me the power, I'm asking you.' Then go to the kitchen silently, so no one notices you or the magic of the words will disappear. Switch on the gas stove, all four burners. But do not light it. You don't want to get burns, do you? Then go to sleep. The magic gas will come to you, you will breathe it while sleeping and in the morning, when you wake up, say: 'Thank you Alfeya, I've become a fairy.' And you will became a real fairy of fire."'

Most likely, no harm will come to Maia, but if her design is successful, she is leveraging the micro:bit to disrupt the power balance in her house, undermining her parents authority with potential negative implications for future interactions. This risk is subtle; but attending to disruptions caused in family dynamics should be a relevant concern for designers, as it may make effective parenting (e.g. rule setting and punishment) more difficult. And while effective parenting is by no means the only barrier protecting children from harm in their digital engagements [33], particularly younger children who rely on parental management of digital risk [12] cannot be supervised during covert IoT device building and use.

The more readily apparent risk is that of invasion of privacy—though this is not a risk to Maia as much as it is a risk to her parents. Certainly if adults were to find out that companies were mining data about their sleep patterns without their permission, there would be an uproar. And if Maia had instrumentalized an audio recorder or camera rather than a pressure sensor the invasion would be all the more glaring. It is important to note, here, that the risks emerging from children's appropriation of IoT are not necessarily isolated to the child user him/herself.

Risks of Assistance

Consistent with other studies (see [13] for summary of works in this area), our data indicates that children ages 9–11 have very little understanding of their own privacy or that of others. This not only manifests in surveillance based uses of the micro:bit, but also in a demonstrable lack of understanding of what constitutes personal data. For example, children did not appear to perceive a substantive difference between collecting data about the number of steps they are taking and collecting data about their steps (or that of others) through time and

[2] The Micro:bit Educational Foundation comprises a number of companies and organizations, including the BBC, working in collaboration (https://microbit.org/about/).

space. This is especially problematic when combined with a lack of understanding about a) the types of data that might be beaconed out by devices (e.g. information about whether a person is in or out of their house), and b) data storage security. To be fully functional, many of the children's designs would require setting up a user profile that is stored on an external server, in which case the risks to the child depend on the often unknown level of security that company has implemented, and the privacy settings a child may consent to without understanding their implications. If intercepted through weak security, activity data might enable a predator to determine a child's present location or predict their future location to orchestrate dangerous face-to-face interactions. It is also possible, and increasingly likely in the future as a market for such services emerges, that companies may offer children easy and free storage of personal data with a view to selling that data on to commercial organizations, or indeed for more nefarious purposes. Finally, we note that the many Assistance technologies that are designed to provide useful instructions to a child—in particular ones that tell them where to go if they are lost—could be hijacked in order to lead a child into dangerous situations.

Troy

Troy is 13 years old, living with his parents and younger siblings (sister, Asia, 11; brother, Lucas, 9). He is constantly getting annoyed with his younger siblings invading his space. For his birthday, Troy's parents got him a small shed at the bottom of the garden that can serve as his own private space away from his siblings. Excited about what they have recently learned about electronics in school, Troy and his three best friends have been using the den as a Maker Space, inventing and programming their micro:bits to make their robots and remote-control cars come to life. They call the shed their "clubhouse" and hold secret club meetings where they discuss their inventions.

Asia frequently interrupts the club's meetings; and Lucas sneaked into the clubhouse and broke one of the remote-control cars. Troy and his friends call an emergency meeting to consider ways to stop annoying siblings from entering the den. They consider special locks but decide it would be more effective to teach them a lesson, so they instead design a way to deliver a small shock to intruders. Their final design uses two micro:bits and fine wire; mains power is connected to an electromagnetic relay system; and the micro:bit's radio buttons A and B trigger the on/off command to arm/disarm the door.

Lucas gets shocked trying to enter the shed and comes crying to Asia, who then marches to the shed, knocks on the door, and informs Troy that if they do that again she will tell their mother what they have been doing. As a counter measure, Troy and his friends decide they need to get some dirt on Asia, so they set up a secret video recorder in her room using a Raspberry Pi, a Raspberry Pi camera module, a PIR motion sensor module and 3 female-to-female jumper wires. At their next secret meeting, they watch what Asia is doing on the camera and make fun of her when she picks her nose. When Lucas gets shocked again and Asia tells Troy she is going to tattle on him, he explains that they have tape of her, and if she does, they will post a video of her picking her nose for all of her friends to see.

Risks to Troy (and his siblings)

Health and safety issues arise in both the build and implementation stages of Troy's design. A tool that can trigger an electric current to shock someone is an alarming and dangerous concept, perhaps especially so when the recipient is a child. Making it more dangerous, even if Troy had experimented with this type of device in other settings, he may not have the know-how to understand potential differences in the voltage of the mains power to his shed which could be high enough to cause serious injury. And for Troy, although the device is relatively simple to make, there is an obvious risk of accidental shocking.

The device that Troy and his friends set up is rigged to deliver a shock when someone touches the door, as opposed to Troy having to press a button to administer the shock. This is significant: since the punishment to Lucas is mediated passively through the device it is likely easier for Troy to psychologically distance himself from the act (it would be much less likely that he would tase his brother, for example). Troy also demonstrates how quickly pranking behavior can escalate, both in terms of physical risk and psychological impact. He uses the device to gain access to places he would normally not be allowed, and then uses that access to violate Asia's privacy and wield control over her in a bullying manner. He also leverages the door handle shocking device in ways that may be subtly bullying, i.e. to enforce social in-groups and out-groups. This feels normal enough as a sibling dynamic, but would more readily be understood as peer-to-peer bullying in, say, a school setting. Finally, if indeed Troy does post the video of Asia for her friends to see, this could lead to cyber bullying and online humiliation (see [21]).

Risks of Play

Most designs that fall into the Play category are not designed to cause a victim physical harm, so it may be difficult for children to understand when and how their device creations negatively affect those around them. And because Play category designs lend themselves most readily to use by a group of children, pack mentality, peer pressure and collective exuberance can increase the likelihood of getting carried away to the point of causing real harm. The 2017 Snapchat challenge "Letter X" is an example of this. The game encouraged children to post "the most vile abuse possible" regarding other children's physical appearance and personality, with others then piling on with further insults [26].

Where devices afford a physical distancing between actions and consequences, this could further heighten vulnerability to health and safety risks to oneself and others. When technologies allow children to conduct themselves without fear of punishment, trolling behavior is likely to thrive; so too is illegal activity, from minor infractions and petty crimes to more serious criminality.

A final risk of Play is the threat of predators making contact with and grooming young people. As places where children congregate to share ideas, predators might taking advantage of IoT Maker forums to access children [10, 32]. For example, concerns have been raised regarding the sexualizing of young children through the game Habbo Hotel, in which teenagers were taking part in online sexual relationships [3]; and Minecraft forums have been used by pedophiles to groom children [20].

Freya

Freya is twelve years old. Her father has left the family and she misses a male role model. Her mother is busy with the other younger children and work, so Freya spends much of her time in her bedroom on computers and has recently expanded her interest to include making and tinkering with gadgets. She is often lonely and has become withdrawn due to some recent incidents of having been bullied.

Freya has discovered online forums and YouTube videos on how to make and build physical computing concepts. She built her first interactive toy—a teddy bear that opened and closed its mouth using a micro:bit and servos—by following instructions provided to her in an online forum. For her next attempt, she followed online guidance to connect an audio interface, including a microphone and speaker into her soft toy shark, and with the code supplied by a forum contributor she was able to program the speech interface that enabled her to ask Sharkie a question and get a response. The device consists of a micro:bit, microphone and speakers, and uses blocks from an unlicensed code library extension to connect to Internet speech recognition and a search engine to return and speak back results.

Freya became friendly with an online persona, IoTFriend, who helped her design and develop IoT devices. Chatting frequently, IoTFriend has become her confidant, offering emotional support about the breakup of her family and advice about how to handle bullies. IoTFriend asked for Freya's address to send her the equipment to build a GPS tracker into her connected toy, so if she was being bullied IoTFriend would be able to rescue her wherever she was. IoTFriend sent Freya a Raspberry Pi, SD Card, Wi-Fi Adapter and GPS USB dongle. The coding and build was complex and required the knowledge of an advanced Maker. However, she had IoTFriend to provide code online, offer her step-by-step tutorials and chat her through the process. Freya now takes Sharkie with her everywhere in case she needs rescuing.

Risks to Freya

It would not take long for a predator to identify Freya as particularly vulnerable to manipulation by asking simple questions about why she wants to build an IoT toy; and predators could easily draw vulnerable children to them by use of temptingly titled instructions, e.g. "How to build a toy that plays with you when you are lonely." Children like Freya are increasingly adept at finding How-To resources online, but may not understand that the instructions they find online are not necessarily safe to follow. In Freya's case, the instructions she was given by someone she learned to trust directed her to construct the means by which a predator could make physical contact to kidnap or otherwise harm her. Even without the use of GPS, if a child walks around with a soft toy that incorporates a device that broadcasts wifi signals or Bluetooth packets, it hunts for a wifi playstation and broadcasts IDs, which can be used to track a child's patterns of activity to assist a predator in intercepting the child.

Finally, even if we assume good intentions on the part of IoTFriend, there is no assurance that IoTFriend is sufficiently knowledgable of privacy and security risks they may be introducing through the code they are passing on to other users—or indeed that it is a child who would end up using the code. The My Friend Cayla doll is a good example of how easy it is to do privacy and security wrong. This IoT toy doll was made famous on account of being banned in Germany under legislation that classifies it as an espionage device [19]. Technically the doll is extremely simple and is based around a Bluetooth microphone/speaker embedded inside an otherwise normal plastic doll, with the microphone and speaker being driven from a supporting mobile app. The doll uses a combination of local processing and supporting cloud services to deliver a range of functions such as storytelling, gaming, and chat. The audio recordings, along with other data captured by the doll, are not confined to the smartphone but are sent via remote servers belonging to the doll manufacturer, where they are subsequently shared with another company who provide the voice recognition service. The doll is also insecure; the Bluetooth connection can easily be hijacked which would provide an attacker full control over the audio data the doll records, as well as what it says. Furthermore, the database that supports the dolls functions—an implementation of SQLite within the doll's smartphone app—was originally not encrypted and hence all the doll's scripted chat responses, including a list of banned words, could easily be tampered with. Subsequent versions encrypted the database but left the decryption key vulnerable. Finally, requests that were passed from the smartphone software to the web, which were not encrypted and sent in plaintext, were relatively easy to intercept.

Risks of Companionship

Our data indicates a clear desire among children to seek emotional support from IoT technologies, seemingly particularly true for girls. As Freya demonstrates, children may volunteer information in ways they are taught not to in online safety education (such as it is) if they are tapping into a culture of collaboration and exchange that is demonstrably productive, i.e. leads to them being able to build technologies that work. But it is important to note that it is technically feasible—if not today, in the next 2-3 years—for children to satisfy a desire for emotional responsiveness in remedial ways (e.g. using A and B radio buttons to indicate happy or sad; getting personalized Alexa-type responses based on prior reactions) that, if intercepted, would enable a predator to time their interactions to moments of peak vulnerability. The more sophisticated the backend technologies children may incorporate into their devices become in terms of providing human-like responses, the more difficult it will be for children to distinguish between a digital interaction they are having through a device and a human interaction they are having with an entity who has hijacked their device.[3] Critically, once an emotional bond has

[3] For examples of toys that have been successfully hacked and hijacked, see [7].

been established between child and device, if that device has been hijacked a child is easily influenced and manipulated to undertake risky behaviors.

GUIDING QUESTIONS

In considering ethical design of IoT technologies, designers face the unique challenge of considering not only human-to-device interactions, but also the implications of "inter-machine chatter" [15] and the consequences of the indirect interactions one might have with various individuals, organizations and services. IoT for children brings into focus the risks associated with peer-to-peer abuse, unknown adult abuse (i.e. by strangers), and known adult abuse (e.g. by relatives, teachers, coaches); as well as the risks of radicalization, unethical commercial exploitation of children's data, and improper management of identifying information about children.

Determining the full extent of risks to children when they programme IoT devices will require the development of some means of accounting for the "ecologies" [1] (see also [29]) in which the consequences of children's own device creations play out. One possible route towards improving thinking in this area is to develop a set of questions to consider as part of one's development process, as per the EthicalOS (ethicalos.org) risk mitigation checklist, which was developed to help tech companies predict the consequences of their products and "avert ethical disasters" [24]. The EthicalOS collaboration has produced a toolkit, a risk mitigation checklist and a number of use cases, but not a readily apparent methodology for generating these outputs to predict consequences of technologies in other contexts. Note that while there are similarities between ours and the EthicalOS project, our methodology was developed independent of EthicalOS and only later borrowed the structure of the risk mitigation checklist and risk zones.

We present below a set of questions that emerged directly from the use scenarios we have described above. To translate these scenarios to guiding questions, we adopted an inductive coding approach. Our process was as follows:

1. We re-read the use scenarios (including the narrative, the discussion of risks to the fictional child, and the discussion of risks from the category of use) and identified particular aspects that contributed to risk until we reached saturation;
2. For each of these risks, we wrote a brief description of the issue (e.g. "undermines parental authority", "parents are unaware", "emotionally vulnerable child");
3. We then conducted a clustering exercise, assigning provisional headings to emerging categories, and reorganizing until satisfied with the groupings and Risk Zone titles;
4. Finally, we reworded the identified issues in the form of questions.

Risk Zone 1: Authority and Discipline

- Will the technology undermine authority, and what might the consequences of this be?
- What might the technology enable children to see or do that they haven't been able to before? Are carers or other authority figures aware the child has these new capabilities? If not, would they approve if they were to find out?
- Does the technology afford covert interactions? Is it important that others are able to tell when a child is using the technology?
- Does the technology enable a child to escape punishment for something they would otherwise be punished for? What risky behavior might children engage in as a result that they otherwise wouldn't?
- Does use of the technology need to be supervised? How likely is it that an adult would be able to supervise this activity? Would that supervising adult be sufficiently knowledgable to protect the child from risks?

Risk Zone 2: Malevolence and Accidental Harm

- How might the technology or data produced by it be used by a malevolent actor? Is there any way to identify malevolent users? How will malevolent users be policed?
- For any given use of the technology, what would it look like if a user 'took it too far'?
- Are those with whom a user interacts able to determine that user is a child? What are the risks of those entities knowing they are interacting with a child? What are the risks of those entities not knowing?

Risk Zone 3: Emotionality and Socialization

- Does the technology appeal to emotionally vulnerable children? If so, how might the technology exacerbate these vulnerabilities?
- Does the technology isolate children? If designed differently, how might it foster real world socialization?
- What emotional state does the technology foster? Is this conducive to deliberation and responsible decision making?

Risk Zone 4: Governance and Accounting

- Will people be producing content or components that extend the original functionality of the technology? How will these individuals and content/components be vetted?
- What tools and services would users interact with as part of normal use of the technology (e.g. servers)? Is it preferable and possible to build a secure ecosystem that supports interaction from start to finish?
- Is it obvious to a child when they are generating data and where it is going? Is this information presented in a way that promotes informed consent?

LIMITATIONS AND FUTURE WORK

Use Scenarios

Representativeness

We are conscious that our methods for eliciting desired uses of the micro:bit may preclude some of the most problematic of children's actual desired uses. The engagement days were supervised by teachers and delivered within the context of an educational field trip. Children were primed to think of academically worthy uses of the technology, in particular ones that demonstrated they had learned something from the morning's instruction.[4] It is likely that they were also censoring ideas that they thought their teachers would not approve of, which otherwise they would happily program in their bedrooms. We glimpsed a darker design instinct in one of the designs from Engagement Day 1: A child had proposed to his friends the idea of a (President) Trump-Seeking Missile, but was scolded by his teacher and forced to develop a more appropriate idea.

We suspect that this self-censorship significantly shaped the distribution of designs across the three use categories—not only for our engagement day data but also for desk research data, as children are unlikely to post ideas online that they know they will get in trouble for. Play is an integral part of childhood and therefore Play seems a natural use of the micro:bit. The percentage of design ideas that fall into the Assistance category may also reflect children's difficulties with imaginative tasks, as they often replicated devices they had seen elsewhere. On the other hand, Assistance uses of the micro:bit are arguably the most realistically implementable, so when children were imagining more creative uses it is less likely they would be able to realize these designs.

While further research is needed to validate this assumption, we believe that children could have darker fantasies for how they might harness IoT technologies, but that they largely lack the skill set to implement such ideas. This may not hold, however, as additional resources become available through adult-driven forums and How-To videos.

Comprehensiveness

Project partners reported finding the use scenarios highly illuminating as well as a useful format for capturing risks to children from IoT. In their words, they reported finding the scenarios "an effective way of beginning to map some of the child protection challenges that might emerge with the internet of things;" that they "moved [our] thinking along;" and that "as a reality check as a team we should be doing more of these."

That said, our project would have benefited from tighter feedback between the us and the project partners during the development of the use scenarios. In particular, we are aware that our understanding of predatory behavior (their area of expertise) is somewhat lacking, and as such there are contexts of abuse that are not accounted for by these use scenarios, e.g. abuse by adults who are known to the child. Although as of yet there have not been any publicized cases of connected toys being used as a tools for known-adult abuse, cases have started to emerge of IoT technologies within the home being weaponized as tools for power and manipulation against domestic abuse victims [31]. Technologies within the home have been used to scare, intimidate, monitor and confuse victims of domestic abuse. Often victims have little or no knowledge of the data collected by the device, or are unaware that the known perpetrator is controlling the device. IoT devices for children could be appropriated for the purposes of manipulation, monitoring and gaslighting, becoming a secret weapon against a child. Further use scenarios are needed to help circumscribe the risks of known-adult abuse through IoT for children.

Usefulness

We recognize that the use scenarios we have provided in this paper are examples of rudimentary implementations of IoT at best, and that the risks they point to are relatively mild. Nonetheless, the scenarios were highly generative of questions that are worthy of consideration not merely to attend to the minor risks represented in the use scenarios but also to more serious risks that could emerge in, for example, more advanced uses of IoT by children. In this sense, an extra step might be useful for future work where the Risk Mitigation Checklist is used to generate a final set of higher risk use scenarios.

Our work might further have benefited from better engagement with risk management literature in helping us appropriately weigh credibility, likelihood and impact in understanding the risk landscape [2, 14]. Going forward, explicating these dimensions might help in evaluating which components of the micro:bit ought to be locked down and which can be left open.

Guiding questions

Additional Considerations

We were particularly struck by the fact that many of the desired uses of IoT we described in our use scenarios should, to an adult, seem immediately problematic; however, it was clear from our Engagement Workshops that children do not readily perceive ethical issues their designs raise. Most obviously, children often produced designs that adults would view as major violations of others' privacy, e.g. surveillance based uses of the micro:bit. This is in keeping with theories of typical moral development: Children in the age group we sampled, who incidentally are just starting to receive computer programming education through their schools, tend to display pre-conventional morality [11]. This developmental level is comprised of two stages that an individual progresses through in sequence, both of which are characterized by an egocentric focus on the direct consequences of actions, as enforced by a moral authority (e.g. a parent, a teacher). In Stage 1, a child understands when they have done something wrong because they are punished. In Stage 2, a child determines right and wrong in terms of their own best interest, without regard for the consequences to others.

The three use scenarios we present illustrate this level of moral development in action. Maia's designs enabled her to escape punishment for something that she would be punished for if she had been seen doing it, thereby (in her mind), making the behavior acceptable. Further, Maia's design may have violated her mother's privacy, but she was preoccupied by her own end goal without consideration of potential consequences to her mother. Similarly, Troy violates Asia's privacy as part of a plan to ensure that he escapes punishment for his prior crime. And as Freya demonstrates, adults are perceived more trustworthy than they perhaps deserve by virtue of being representative of the moral authorities children are used to listening to in order to avoid punishment.

[4] Notably, the 10- to 11-year-olds were much more preoccupied with demonstrating learning than the 9- to 10-year-olds, e.g. asking whether their designs needed to include instructions for building the device.

It is important that developers and policymakers take children's level of moral development into account. One cannot assume that children are able to grasp and internalize right and wrong in a way familiar to adults. As such, many of the questions require the developer or policymaker to interpret risk through the lens of a child's limited capacity for moral behavior; and additional structures may need to be provided within a given tool to actively guide children toward ethical use.

Validating the Checklist

Future work will seek to refine and validate our Risk Mitigation Checklist through a series of interviews with experts in both IoT and predatory behavior. These interviews will focus on the novelty and comprehensiveness of the insights generated through this methodology, i.e. what they learned that they did not know already, how it mapped onto their list of known concerns, and (for The Micro:bit Educational Foundation consortium) how it compared with their own thought processes in developing IoT for children. We will also explore how, at what stage(s) in the design process, and to what end our informants think they might make use of this Checklist; as well as the limitations of the Checklist in attending to risks that derive from underlying (non-technical) issues, such as parental oversight. And finally, we will look to emerging high profile failures of IoT for children as evidence of the importance of asking specific questions included in this Checklist.

CONCLUSION

In this paper we have described a methodology designed to elicit privacy, security and safety risks of children programming Internet of Things devices such as the BBC micro:bit. Using a drawing-telling technique to generate data regarding children's desired uses of the micro:bit, we were able to identify three broad categories of use which circumscribe distinct sets of risks to children. We made these risks tangible by creating narrative use scenarios, and then used these scenarios to generate practical questions that developers and policymakers can ask in creating and evaluating IoT for children.

Having been forthcoming regarding potential limitations of the methodology, it is important to convey what we believe the main successes of the methodology are. Principally, it has helped formalize the process of designing out risk—a process that organizations such as the BBC already tacitly conduct. Certainly, the majority (if not all) of the risks we have identified through our methodology were previously known to the makers of the micro:bit, but there are three advantages of having arrived at them via this process. Firstly, direct participant engagement helped ensure that *actual* likely uses and associated risks are explored, beyond what adults imagined children might want to do with the technology. Secondly, the methodology helped validate the micro:bit's developers' thinking and assuaged fears about possible unknown risks that had forced them to proactively limit functionality. Thirdly, and most tangibly, it provides a toolset (the Risk Mitigation Checklist) that they and others might use to ensure they do due diligence in developing a device that is safe for children. The scenarios themselves, which describe fairly tame problem uses, are not as inherently useful as they are generative for eliciting salient design considerations.

ACKNOWLEDGMENTS

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 organize 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] Susanne Bødker. 2006. When second wave HCI meets third wave challenges. In *Proceedings of the 4th Nordic conference on Human-computer interaction: changing roles*. ACM, 1–8.

[2] Hervé Borrion and Noémie Bouhana. 2012. iCARE: A Scenario-Based Method for the RIBS Project. In *2012 European Intelligence and Security Informatics Conference*. IEEE, 284–284.

[3] J. Carr. 2012. Viewpoint: What went wrong at Habbo Hotel? https://www.bbc.co.uk/news/technology-18433471. (2012).

[4] Audrey Desjardins and Ron Wakkary. 2011. How children represent sustainability in the home. In *Proceedings of the 10th International Conference on Interaction Design and Children*. ACM, 37–45.

[5] Allison Druin. 1999. *The Role of Children in the Design Technology*. Technical Report.

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

[7] Family Online Safety Institute. 2016b. 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. (2016).

[8] 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).

[9] Daniel Fitton and Janet C Read. 2016. Primed Design Activities: Scaffolding Young Designers During Ideation. In *Proceedings of the 9th Nordic Conference on Human-Computer Interaction*. ACM, 50.

[10] Emily A Greene-Colozzi. 2017. An Exploration of Youth Experiences in Chatrooms. http://tinyurl.com/y4lt8y99. (2017).

[11] Lawrence Kohlberg and Richard H Hersh. 1977. Moral development: A review of the theory. *Theory into practice* 16, 2 (1977), 53–59.

[12] Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L Clegg, and Jessica Vitak. 2017. 'No Telling Passcodes Out Because They're Private': Understanding Children's Mental Models of Privacy and Security Online. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 64.

[13] Priya Kumar, Jessica Vitak, Marshini Chetty, Tamara L Clegg, Jonathan Yang, Brenna McNally, and Elizabeth Bonsignore. 2018. Co-designing online privacy-related games and stories with children. In *Proceedings of the 17th ACM Conference on Interaction Design and Children*. ACM, 67–79.

[14] Tanya Le Sage, Sonia Toubaline, and Hervé Borrion. 2013. An object-oriented approach for modelling security scenarios. In *2013 UKSim 15th International Conference on Computer Modelling and Simulation*. IEEE, 396–400.

[15] Joseph Lindley, Paul Coulton, and Rachel Cooper. 2017. Why the internet of things needs object orientated ontology. *The Design Journal* 20, sup1 (2017), S2846–S2857.

[16] Andrew Manches, Pauline Duncan, Lydia Plowman, and Shari Sabeti. 2015. Three questions about the Internet of things and children. *TechTrends* 59, 1 (2015), 76–83.

[17] 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.

[18] Neema Moraveji, Jason Li, Jiarong Ding, Patrick O'Kelley, and Suze Woolf. 2007. Comicboarding: using comics as proxies for participatory design with children. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 1371–1374.

[19] BBC News. 2017a. German Parents Told to Destroy Cayla Dolls Over Hacking Fears. https://www.bbc.co.uk/news/world-europe-39002142. (2017).

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

[21] NSPCC. 2016. Sexting: Understanding the Risks. https://www.nspcc.org.uk/globalassets/documents/online-safety/sexting-understanding-the-risks.pdf. (2016).

[22] 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).

[23] Seymour Papert. 1986. *Constructionism: A new opportunity for elementary science education*. Massachusetts Institute of Technology, Media Laboratory, Epistemology and Learning Group.

[24] A. Pardes. 2017. Silicon Valley Writes a Playbook to Help Avert Ethical Disasters. https://www.wired.com/story/ethical-os/. (2017).

[25] James Pierce and Carl DiSalvo. 2017. Dark Clouds, Io&#!+, and [Crystal Ball Emoji]: Projecting Network Anxieties with Alternative Design Metaphors. In *Proceedings of the 2017 Conference on Designing Interactive Systems*. ACM, 1383–1393.

[26] J. Rodger and J. Taylor. 2017. Everything you need to know about the Letter X Snapchat bullying craze. https://www.cambridge-news.co.uk/news/uk-world-news/snapchat-facebook-social-media-bullying-13994981. (2017).

[27] Sue Sentance, Jane Waite, Steve Hodges, Emily MacLeod, and Lucy Yeomans. 2017a. Creating Cool Stuff: Pupils' Experience of the BBC micro:bit. In *Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education*. ACM, 531–536.

[28] Sue Sentance, Jane Waite, Lucy Yeomans, and Emily MacLeod. 2017b. Teaching with physical computing devices: the BBC micro:bit initiative. In *Proceedings of the 12th Workshop on Primary and Secondary Computing Education*. ACM, 87–96.

[29] Rachel C Smith, Ole S Iversen, Thomas Hjermitslev, and Aviaja B Lynggaard. 2013. Towards an ecological inquiry in child-computer interaction. In *Proceedings of the 12th International Conference on Interaction Design and Children*. ACM, 183–192.

[30] W. Stewart. 2017. Five-year-old girl suffers horrific burns after becoming the latest victim of 'fire fairy' game spreading online where children are told to secretly turn on gas rings. https://www.dailymail.co.uk/news/article-4290590/Fire-fairy-game-tells-children-turn-gas-stoves.html. (2017).

[31] The New York Times. 2018. Thermostats, Locks and Lights: Digital Tools of Domestic Abuse. https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html. (2018).

[32] 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.

[33] Pamela Wisniewski. 2018. The Privacy Paradox of Adolescent Online Safety: A Matter of Risk Prevention or Risk Resilience? *IEEE Security & Privacy* 16, 2 (2018), 86–90.

[34] Susan Wright. 2007. Graphic-Narrative Play: Young Children's Authoring through Drawing and Telling. *International Journal of Education & the Arts* 8, 8 (2007), 1–28.