IoT4Kids: Strategies for Mitigating Against Risks of IoT for Children

Bran Knowles
Lancaster University
Lancaster, UK
b.h.knowles1@lancaster.ac.uk

Sophie Beck
Lancaster University
Lancaster, UK
s.beck@lancaster.ac.uk

Georgia Newmarch
Lancaster University
Lancaster, UK
g.newmarch@lancaster.ac.uk

Joe Finney
Lancaster University
Lancaster, UK
j.finney@lancaster.ac.uk

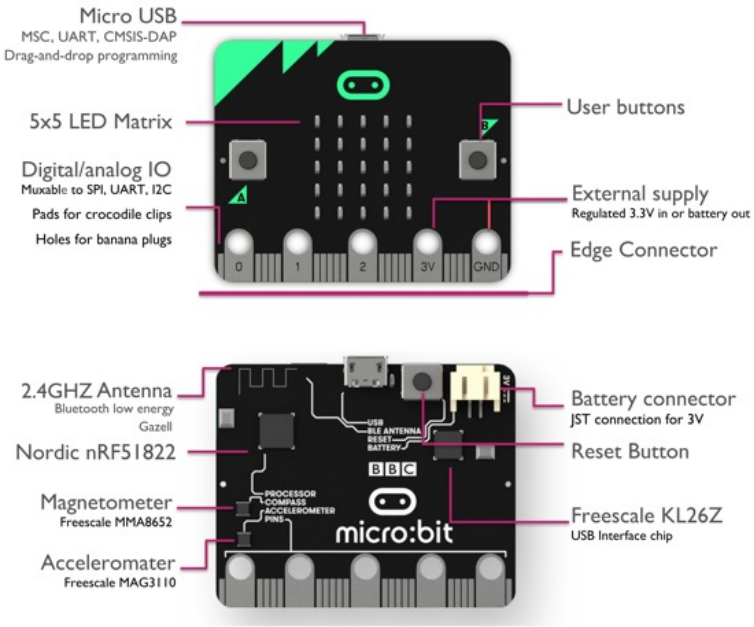
James Devine
Lancaster University
Lancaster, UK
j.devine@lancaster.ac.uk

ABSTRACT

This paper describes the key outputs of IoT4Kids, a project exploring the privacy, security and safety implications of children programming the Internet of Things. We present our Risk Mitigation Checklist in order to illustrate the need for a multi-pronged approach for attending to risks to children from emergent IoT devices, and we discuss what this may mean in terms of industry practice, policymaking and education.

CHI'19 Extended Abstracts, May 4–9, 2019, Glasgow, Scotland UK

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM.
https://doi.org/10.1145/nnnnnnn.nnnnnnn



CCS CONCEPTS

• **Human-centered computing → Human computer interaction (HCI)**;

KEYWORDS

Internet of Things; IoT; children; ethics

ACM Reference Format:
Bran Knowles, Sophie Beck, Georgia Newmarch, Joe Finney, and James Devine. 2019. IoT4Kids: Strategies for Mitigating Against Risks of IoT for Children. In *Proceedings of CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI'19 Extended Abstracts),* Blank, Blank, and Blank (Eds.). ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

INTRODUCTION

The PETRAS Internet of Things Research Hub (https://www.petrashub.org/) was launched in the UK in 2016 to explore privacy (P), ethics (E), trust (T), reliability (R), acceptability (A) and security/safety (S) issues pertaining to the IoT. Among the 40+ projects that are funded through this hub, only one focuses on risks associated with child users of IoT, namely our IoT4Kids project. This project was motivated by uncertainties surrounding the privacy, security and safety implications of the BBC micro:bit, a handheld programmable IoT device designed for children (see image left and visit microbit.org for more details). Concerns regarding unknown risks arising from the device prompted its developers to limit its functionality: they restricted some functions like those involved with radio communication, strengthened security around others such as Bluetooth pairing, and limited its use to safe educational (closed) environments. Such caution in launching the device is laudible (and perhaps rare); but more information was needed regarding the actual risks children might face when doing rudimentary programming of the IoT in order to determine whether such measures were necessary or appropriate.

The goal of the IoT4Kids project was to produce guidelines for developing safe, ethical IoT devices for children. Ultimately the project found that addressing risks to children in this space will require a multi-pronged approach that attends not only to industry practices, but also to policymaking and education. In this paper we present our Risk Mitigation Checklist and discuss how it pertains to these three strategic areas.

METHODS AND FINDINGS

The IoT4Kids project had three aims corresponding to three stages of research, now completed. Details about our methods and findings are currently in submission, but we provide a summary below.

Aim 1: *To understand the potential applications of BBC micro:bit as a programmable IoT platform for children in order to anticipate a range of scenarios which may present different challenges in terms of privacy and security.*

Stage 1: Outreach days were held with children (ages 9-11), in order to explore how they might use devices such as the micro:bit [5]. Children were provided micro:bits, given a tutorial on how to use the device, and guided through a creative exercise to elicit their ideas for exciting uses of the micro:bit. In this exercise, children first worked in teams to generate a number of ideas of what they could use the micro:bit for; then they worked individually to expand their favorite idea, using a worksheet to sketch and write about their design. The data resulting from this participant engagement was themed into 3 high level types of uses from which different clusters of risk emerge, namely:

- *Assistance:* tools designed to help children complete mundane tasks; e.g. reminder/alarm devices, activity trackers, remote controls, tracking tags for treasured items;
- *Play:* tools designed to simulate activities that children are otherwise unable to experience or forbidden from engaging in; e.g. driving a (real) car remotely, VR simulations, rigging devices to scare siblings;
- *Companionship:* tools designed to provide emotional support and ease loneliness; e.g. interactive dolls and toys.

Risks were explored through the development of Use Scenarios. These were fictional amalgamations of the participants' desired uses of the devices, taking the form of narratives that were crafted to highlight potential privacy and security implications [4].

Aim 2: *To identify current barriers to being able to responsibly deploy micro:bit as an IoT tool for children in order to develop a comprehensive understanding of the potential implications of use of this and similar tools for which design solutions are needed.*

Stage 2: The Use Scenarios developed in Stage 1 were enhanced by information gleaned from our project partners during key informant interviews and partner workshops. The National Society for the Prevention of Cruelty to Children (NSPCC) and the Family Online Safety Institute (FOSI) provided expertise in predatory behaviour to help us anticipate threats to children; and The Micro:bit Educational Foundation provided information regarding the necessary tech components and skills for realizing children's desired uses of the micro:bit, as well as known uses of the tool by children to date. Feedback solicited from these project partners was used to further refine and expand the set of Use Scenarios (details to be published in [1]).

Aim 3: *To elaborate a series of compelling use scenarios which illuminate important privacy and security implications in order to develop guidelines for development of acceptable programmable IoT devices for children.*

Stage 3: The resulting Use Scenarios were then used as a basis from which to derive questions that should be asked to help mitigate against the risks identified in the scenarios. These questions were categorized into four Risk Zones: 1) Authority and Discipline; 2) Malevolence and Accidental Harm; 3) Emotionality and Socialization; and 4) Governance and Accounting. These Risk Zones and guiding questions therein comprise the Risk Mitigation Checklist - a concept borrowed from the EthicalOS project (https://ethicalos.org/). The Checklist is intended as a tool to be used by developers, policymakers and educators to anticipate and proactively attend to risks of IoT technologies [4].

Risk Mitigation Checklist

We present below the categories of risks we identified through our process, and the questions we think are salient to the context of developing IoT for children.

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?

DISCUSSION

We contend that consideration of the questions above is the responsibility not only of those developing technology, but industry more widely, policymakers, and educators. We expand below.

Industry Practice. Development of the micro: bit was led by the BBC, who by virtue of their charter, have a duty to the public that requires they carefully consider the ethical implications of their activities. Ideally other companies would take such a considered approach, and it may be that formalising an ethical design process for industry removes one of the barriers to doing so. The Checklist is one formal framework that could be developed further for wide use by industry, and while we have provided some initial questions, we believe garnering buy-in from industry will require a consortium of leading companies to generate a similar framework.

Policymaking. Currently, while the GDPR regulates protective measures regarding children, there remains a challenge of obtaining informed consent from child users: e.g. is the child or parent responsible for consenting [6]? We also note that governance of IoT toys, for example, is framed as the responsibility of parents rather than a problem to be dealt with through legislation and policy [3]. Given the pace of technological change, appropriate policies legislating IoT need to be reviewed regularly; indeed, a process for regularly reviewing these requirements may need to be developed.

Education. Schools currently play a key role in delivering online safety education [2], and organizations such as the NSPCC and FOSI also provide materials to support schools, parents and children in raising

awareness and education on online safety (see https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/ and https://www.fosi.org/). These materials, along with school curricula, have not yet caught up with the new contexts of IoT toys and programmable IOT.

CONCLUSION

The next steps for our work are to a) solicit feedback from our project partners on the usefulness of the Risk Mitigation Checklist and iterate the list as appropriate; b) explore strategies for involving children in the design process towards developing next generation programmable IoT tools; and c) drawing inspiration from the risks identified in IoT4Kids to deliver tangible micro:bit based lessons in the form of 'workshops-in-a-box': fun, interactive, packagable IoT safety teaching resources for primary school classrooms. Our interest in attending the New Directions for the IoT workshop is to work with fellow researchers, designers and practitioners to better understand the trajectory of IoT—what can we expect the IoT to become in the near and distant future? This would be invaluable experience for advancing our thinking to a) anticipate additional risks to children and b) conceive of new ways of responsibly capitalizing on the potential of IoT technology.

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).

REFERENCES

[1] Sophie Beck, Bran Knowles, and Joe Finney. [n. d.]. Exploring the Risks of Children Engaging with Programmable IoT. *Forthcoming*.

[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.

[3] Melanie L Hersh. 2000. Is Coppa a Cop Out-The Child Online Privacy Protection Act as Proof That Parents, Not Government, Should Be Protecting Children's Interests on the Internet. *Fordham Urb. LJ* 28 (2000), 1831.

[4] Bran Knowles, Joe Finney, Sophie Beck, and James Devine. [n. d.]. A Methodology for Designing Out IoT Risks to Children. *In submission*.

[5] Bran Knowles, Joe Finney, Sophie Beck, and James Devine. 2018. What children's imagined uses of the BBC micro: bit tells us about designing for their IoT privacy, security and safety. In *PETRAS Living in the Internet of Things '18*. IET.

[6] Lydia Plowman. 2015. Researching young children's everyday uses of technology in the family home. *Interacting with Computers* 27, 1 (2015), 36–46.