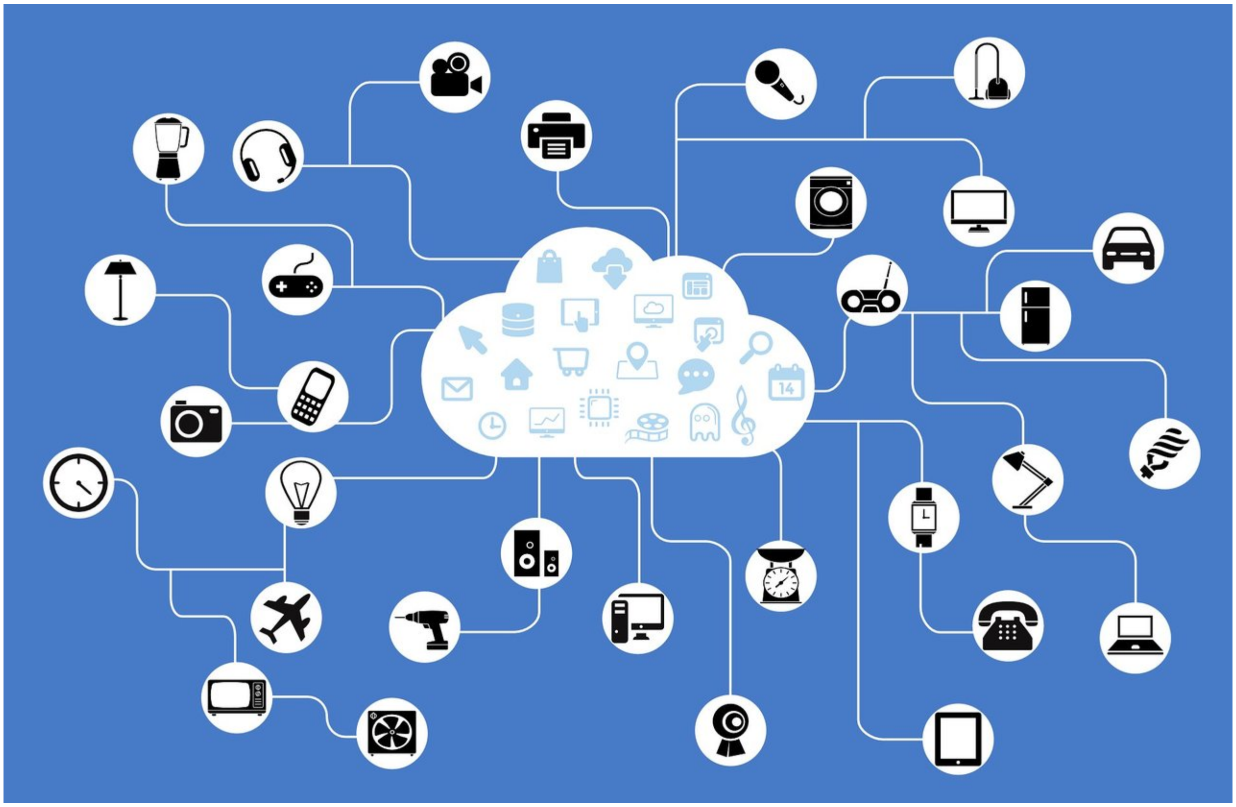
Keeping children safe in the 'Internet of Things' age

June 21 2019



Credit: CC0 Public Domain

Children need protection when using programmable Internet computing devices—and Lancaster University scientists have drawn up new guidelines to help designers build in safeguards.

Young people are growing up in a digital world where everyday objects contain sensors and stream data to and from the Internet—a trend known collectively as the Internet of Things (IoT).

Children are also getting hands-on—using small-scale easy-to-program devices such as the BBC micro:bit to experiment and get creative with digital technologies.

These kinds of devices are very useful educational tools that children are using to build their knowledge and digital skills—and the developers of the BBC micro:bit took a very considered ethical approach to developing their device. However, unless properly considered, Internet-connected devices can present risks to children and others around them.

These risks can include peer-to-peer abuse or bullying, dangers of abuse by adults, as well as risks related to the use, exploitation, commercialisation, or insecure management of any data the children generate by using the devices.

Dr. Bran Knowles, Lecturer in Data Science at Lancaster University's School of Computing and Communications, said: "Children who are learning to programme IoT devices still have critical gaps in their understanding of privacy and security. In addition, their parents may also lack technical understanding of IoT, which makes it difficult for them to help ensure their children are managing their privacy and keeping safe.

"Formal training is available for online safety issues such as social media bullying and sexting, but, as yet, there is no IoT component to this curriculum.

"It is essential therefore that the designers of these IoT devices anticipate the full spectrum of contexts in which children may use these devices and adopt strategies that will ensure they have properly considered, and mitigated, the potential safety and privacy risks to children and their families.

"Our research provides a framework to help designers approach these critical risks with their own devices, while still enabling these devices to have enough functions activated so that they still provide a fun learning experience." she said.

The Lancaster University team's methodology includes working with supervised groups of school children to explore a wide range of ways that young people may want to use Internet-connected computing devices.

The findings from these sessions, alongside findings from workshops with child safety experts, help designers to create fictionalised 'use scenarios' that provide a detailed picture of how children will use the devices. Key questions can emerge from these scenarios that form the basis for developing risk mitigation checklists when designing digital tools.

The research is outlined in the paper 'A Scenario-Based Methodology for Exploring Risks: Children and programmable IoT', which is to be presented at the Designing interactive Systems (DIS 2019) conference. The paper has received an 'Honourable Mention for Best Paper' at DIS 2019.

Provided by Lancaster University

Citation: Keeping children safe in the 'Internet of Things' age (2019, June 21) retrieved 26 April 2024 from https://phys.org/news/2019-06-children-safe-internet-age.html