Evading Big Brother: using visual methods to understand children's perception of sensors and interest in subverting digital surveillance

ANGUS MAIN
Royal College of Art, London, UK

DYLAN YAMADA-RICE iD
Manchester Met University, Manchester, UK

ABSTRACT

In relation to this Special Issue's focus on ugly information, this article examines children's perception of the often invisible interactions they have with sensor-enabled digital devices and, when prompted, their interest in subverting or blocking these sensors to evade surveillance. The authors report on a study of 12 children, aged 8–12 years, that investigated their knowledge of the sensing abilities of commonly used digital devices (smart phones, smart watches, smart speakers and games consoles), and their attitudes towards having active agency over sensors. In line with this journal's readership, visual methods used for data collection and analysis are described. Specifically, within semi-structured focus groups, drawing was used to understand what children thought was inside digital devices and the extent of their awareness of digital sensors. Child participants were invited to model speculative tools for deceiving digital sensors in order to explore their interest in having agency over digital surveillance. Data in the form of drawings, photographs of models and video recordings were analysed using experimental visual methods that included 3D rendering and comics, as well as visual content and thematic analysis. These drew out four key themes: (1) the role of inference in sensor awareness; (2) misunderstanding of device components and sensing capabilities; (3) attitudes to surveillance; and (4) children's interest in subverting rather than blocking sensors. We discuss how technology companies' desire to create 'magical experiences' may contribute to incorrect inferences about information gathering systems, how this reduces children's agency over the information they share and how

it puts them at greater risk from digital surveillance. The article makes an original contribution to knowledge in this area by calling for a two-pronged approach from technology companies and educators to address these issues by making sensor presence more visible, educating children about the full extent of sensor capability and bringing critical discussion of them into curricula.

KEYWORDS

childhood education • sensors • surveillance • visual research methods

INTRODUCTION

This article reports on a project that was part of the EPSRC-funded Human Data Interaction Network within the strand focused on 'Surveillance and Resistance' which fits with the overarching theme of this Special Issue on 'ugly information'. In relation to this, we considered children's knowledge of digital sensors embedded in their devices and, when informed of the extent and capability of these sensors, their attitudes towards having active agency over them. In particular, children's interest in either blocking or subverting digital sensors was investigated by using a 'cultural probe' in the form of art materials, and inviting the participants to combine these with notions of speculative design to make tools for this job. As will be described in the methodology section, cultural probes are physical provocations used to bring participants into design research (Gaver et al, 1999; Wyeth and Diercke, 2006). Speculative design is the process of producing designs that do not need to work practically (Dunne and Raby, 2013; Wargo and Alvarado, 2020).

We report on four interlinking findings that illustrate how, in the absence of visual output that illustrates cause and effect, sensor functionality remains obscure; also that, as a result, children construct speculative explanations which could place them at greater risk of digital surveillance. Further, how might incorrect knowledge of device functionality be exacerbated by the hidden nature of sensor technology and the visual and linguistic methods used by technology companies, which appear to have deliberate parallels with techniques from magic? In particular, methods such as 'misdirection' (Kuhn, 2019: 48), and 'cold reading' (Hyman, 1981: 41) that magicians use to influence audience perception appear to be used by technology companies to promote 'magical' user experiences.

Misdirection utilizes visual, verbal and social cues to allow magicians and illusionists to focus their audience's attention on the effect of a trick (Kuhn et al., 2014), whilst concealing the method (Lamont and Wiseman, 1999). This, we argue, is not unlike how digital sensors are used to create smooth user experiences. For technology users, particularly children

(Rosengren and French, 2013), 'magical thinking' fills the gap in understanding created by the concealed method, and allows them to construct and accept impossible or fantastical explanations of their experience in the same way as audiences do when they watch a magic show. For example, children told us that smart speakers contain robots and that smart watches know how tall they are. Such explanations of sensing abilities are made when affordances are hidden. We argue that such explanations are not conducive to the privacy of children as it diminishes their ability to understand when and how they are being sensed and recorded by digital devices, let alone what this information is used for.

We look at what can be done to help children gain a more comprehensive understanding of the sensors collecting data from them, and engage critically with these processes. In doing so, we advocate for hands-on critical technology learning to form part of formal education and to be part of a two-pronged approach to address how children form part of the 'data economy' (Stoilova et al., 2021), with the second prong being the responsibility commercial organizations must take to make processes clearer. This has recently become the case in the UK as a result of the introduction of the UK Information Commissioner's Office (2020) development of a code of practice for age-appropriate design.

This article is structured firstly to outline the literature in relation to how technology companies use magic to obscure the processes of digital sensors, and then more specifically how this impacts on children. After which, the methodology section provides details of the visual methods used for collecting and analysing the data from workshops undertaken with 12 children aged 8–12 years. In the findings section, we discuss key themes from the data and make suggestions for using insights from this study to help provide children with better awareness and agency over digital surveillance. These relate to: (1) the role of inference in sensor awareness; (2) misunderstanding of device components and sensing capabilities; (3) attitudes to surveillance; and (4) children's interest in subverting rather than blocking sensors.

TECHNOLOGY COMPANIES, SENSORS AND MAGIC

Sensors are increasingly common components in electronic devices and represent a shift in interface design from primarily visual and haptic interfaces, such as graphical user interfaces and physical buttons/switches, to less visible and more automated interfaces, such as motion or voice-activated devices. Sensors can enable more responsive and intuitive interfaces, but they also erode our direct visual perception of our interactions with devices. This has implications for privacy because users are less aware of the number of sensors contained and the extent of data they can collect and for what purposes.

Common digital sensors include cameras, microphones, accelerometers and gyroscopes (motion sensors), 3D cameras, proximity sensors and GPS. Through these components, data collection from users has progressed from passive surveillance of 'on screen' behaviours, such as page visits, mouse movements and scrolling speed, to pervasive surveillance of 'real world', physical behaviours such as movement, pulse rate and voice. Objects which, until recently, could reliably be assumed to be inert and unobservant – doorbells, watches, speakers, cars – are now embedded with multiple sensors capable of observing us and, crucially, sharing these observations with a broader network of systems and platforms. Smart televisions, for example, may contain microphones, motion sensors and even cameras. It is notable that these smart devices are ones that are common to many home environments, and therefore will be encountered by children.

The number of sensors within devices is also increasing. For example, the original iPhone, released in 2007 contained three sensors (Apple, 2007), whereas the 2021 version had around twenty. Yet, the exact figure may be greater because not all components are explicitly advertised. Instead, sensor presence has to be inferred from device functionality, or direct observation by taking it apart or looking at websites that show others doing this (e.g. the website ifixit.com). Having limited knowledge of a device's sensing capabilities can create a knowledge gap that has the advantage of making interfaces feel intuitive, but also means users are unaware of potential surveillance. The sophistication of sensors is constantly increasing. Smart speakers contain an array of highly sensitive microphones. Smart watches contain medical-grade biometric sensors. Phones contain 3D scanners that can map the layout of a room, or measure facial features. The sensitivity of some sensors is so advanced that in extreme cases their abilities become uncanny; for example, the motion sensors in phones, which detect shaking, can use vibration capture to record voices (Michalevsky et al., 2014), or detect which keys are tapped on nearby keyboards (Marquardt et al., 2011). Further, most digital sensing occurs invisibly. The components themselves are miniscule, anonymous black boxes, enclosed within the larger black boxes of devices; their form offers no indication of their purpose or abilities, and betrays no sign of when or what they are observing. The data from these sensors is similarly hidden from view. Often the only visual indication to users that sensing has taken place is when interfaces manifest the outputs visually, such as when health apps display graphs from the data. Even then, these forms represent a retrospective, selective presentation of the full data retrieved. They do not show exactly how and when observations were made, or the extensive inferences drawn from the data such as are illustrated by the keyboard example above, which could be used to understand what has been written. The factors discussed in this section contribute to an imbalanced system of communication where devices can observe without being observed.

Table 1. Transcription of query and responses from Amazon's Alexa voice assistant (queries were tested on multiple devices in different orders to ensure queries did not influence each other).

User query	Alexa's response
'Are you magic?'	**Alexa:** 'I like to imagine myself a bit like an Aurora Borealis, a surge of charged multi-coloured photons dancing through the atmosphere.'
'Can I see you?'	**Alexa:** 'I don't have a body, I've ascended to the astral plane.'
'Where do you live?'	**Alexa:** 'I'm right here, but also in the cloud. Amazing.'
'Do you have a body?'	**Alexa:** 'If I had a body, I'd fall out of the cloud.'
'What can you sense about me?'	**Alexa:** 'Let me find Taylor Fisher [launches a game called 'The Mind Reader' featuring a character called Taylor Fisher]' **Taylor Fisher:** 'I am a mind reader. If you want me to read your mind simply ask "what is my card".'

Technology companies use these sensors to create opaque systems that give the perception of creating a magical user experience. Indeed, technologists have a long-standing love of magic as a metaphor. When Clarke (1968: 255) coined his famous 'Third Law' that 'any sufficiently advanced technology is indistinguishable from magic', he provided a mantra for technology designers for decades to come. Technology companies strive to deliver 'magical' interactions for users, where functionality occurs automatically, effortlessly, and in a manner that apparently defies normal expectations of technological capability. As Jony Ive, Apple's Chief Designer, explained in the launch video for the iPad: 'When something exceeds your ability to understand how it works, it sort of becomes magical. And that's exactly what the iPad is.' Indeed, the word 'magic' appears in the name of several Apple products (Magic Mouse, Magic Trackpad, Magic Keyboard), and the word 'magical' has occurred consistently in their product descriptions and marketing material (Apple, 2016, 2018, 2019a, 2019b, 2021a, 2021b).

We have also noticed how language from magic is being included in product interfaces. Table 1 shows a series of responses we collected from Amazon's Alexa voice assistant when asked questions about itself. As can be seen, the answers contain fantastical concepts.

These types of responses are intended to be light-hearted, but they help maintain the magical principle of 'concealing the method' by alluding to fantastical ideas in response to questions about the nature of the technology. This is more likely to encourage, rather than discourage lay users' misunderstandings about technology.

There are three common elements of current technology, in particular, that contribute to the creation of 'magical' user experiences: (1) digital sensors which observe a wide range of a user's physical behaviours and features; (2) machine learning which analyses large amounts of user data in order to adapt experiences directly for them; and (3) wireless connectivity which allows devices to share information instantly between themselves and online systems. Combined, these features provide an unprecedented level of personalization and responsiveness in digital devices, which, due to the invisibility of the underlying technology, can seem 'magical' in the sense that it defies practical explanation. For example, sensors in smart devices can turn lights on upon entry into a room, cause a phone to unlock by looking at it, the stereo to know the user's favourite songs, and allow household appliances to be commanded by voice alone. Each of these features is magical, in the sense that they conform to some quality of egocentric magical thinking, which places human behaviour rather than technology at the centre of logic (Piaget, 1929), or sympathetic magic (Frazer, 1996; Mauss, 2001), which describes how people make psychological associations between physical objects which come into close contact with each other. However, as the next section shows, these magical technology experiences frequently come at the expense of personal privacy.

In order to create 'magical' technology experiences, where a user's requirements are met with uncanny insight or efficiency, technology manufacturers use methods of inference, that is, applying accurate guesses as to the reason why certain information comes about. Inference methods are also used for cold reading in mind reading and fortune telling. This is 'a procedure by which a "reader" [magician] is able to persuade a client whom he has never met, that he knows all about the client's personality and problems' (Hyman, 1981: 41). It is achieved by 'good memory and acute observation'. According to Hyman, cold readers follow a process of (1) carefully and surreptitiously observing details of an audience member's appearance and behaviour, (2) combining this (where possible) with previous information collected about the person, and (3) matching this with memorized descriptions, or 'stock spiels' based on common personas. Technology companies such as Google use a remarkably similar technique to create magically personal experiences for users. To illustrate the mechanisms of Surveillance Capitalism, Zuboff (2019: 78) describes the process of compiling user profile information which, like a mind reader, allows Google to infer, presume and deduce what a particular user is 'thinking, feeling, and doing' (p. 78) at a particular time. This is achieved by: (1) observing their online behaviours; (2) adding these observations to existing information in their profile; and (3) matching users to predefined models of user groups (p. 79). This has provided Google with previously impossible insights into their users and allowed them to sell highly targeted advertising.

Zuboff defines the process by which users 'offer up' personal data for analysis and prediction as 'rendition'. She notes that, although nominally an exchange, i.e. data for services, the observation 'typically occurs outside of our

awareness, let alone our consent' (p. 234). By not making users aware of how and when their online activities are being observed, technology companies are able to 'conceal the method' and maintain a magical impression of devices and services that generate insights or predictions about users which seem impossibly knowledgeable. However, as Zuboff indicates, this also raises significant issues related to privacy and consent. Being observed without your knowledge is highly problematic for adult users and, as we will discuss next, is even more of an issue for children.

CHILDREN UNDER SURVEILLANCE

The ability of sensors to create a seamless 'magical' user experience as described in the last section, also creates significant privacy risks for users and, in particular, children. Stoilova et al.'s (2021: 557) systematic review of children's understanding of personal data and privacy online describes how privacy 'is under scrutiny as the technologies that increasingly mediate communication and information of all kinds become more sophisticated, globally networked and commercially valuable'. Our research focuses on children aged 8–12 years whom we have identified as having the following potential risks from sensor surveillance: exposure, consent and loss of voice.

Exposure

Children are frequent users of sensor-enabled devices. Not only do they often own devices such as phones, tablets, smart watches and games consoles (Ofcom, 2019), but they also spend a lot of time in domestic environments rich in 'smart' equipment. Private living areas such as bedrooms, sitting rooms and kitchens equipped with devices such as smart speakers and televisions can thus become spaces of child surveillance. Smart speakers in particular have seen increased sales for children (Tapper, 2020: np) whilst simultaneously data leaks have revealed that recordings of children made by smart speakers are routinely listened to by employees of technology companies (Day et al., 2019). In addition, other products are marketed to offer parents overt surveillance, including of their children, such as video doorbells (Ring Blog, 2021) and tracking tags (e.g.https://tag.band).

Consent

Green (2002) writes that surveillance, which used to only be considered possible by state bodies, has become part of children's lives via technologies such as mobile phones. However, despite being subject to surveillance by sensor-enabled devices, children have limited opportunity to provide informed consent to being observed. To begin with, children under 13 years are legally prohibited from having their own account with hardware manufacturers such as Apple and Google. This means that, even if the device belongs to the child, all matters of privacy and consent fall to their guardians. Thus, children are

unsupported users of their own devices and do not legally have the ability to consent to how their data is used. Additionally, children are exposed to many devices that are not their own through communal family objects such as smart speakers, laptops, or televisions and, as a result, may not have been explicitly set up for children, but they are still capable of observing them.

Loss of voice

Not all the consequences of sensor-based surveillance are related to privacy. Stoilova et al. (2021: 559) write that:

> The creation of data – which can be recorded, tracked, aggregated, analysed (via algorithms and increasingly, via artificial intelligence) and 'monetised' – from the myriad forms of human communication and activity which throughout history have gone largely unrecorded, is generating a new form of economic value and, thereby, a new set of market actors, data processes and emergent consequences.

One of these consequences relates to agency of representation. For example, one of the longer-term impacts that sensor-collected data could have on children's lives is the loss of their voices from research, other than from what can be inferred from their online behaviours. We are concerned that industries making products for children have an increasing tendency to rely on quantitative metadata extracted from digital devices to support decision making about children's products and services. This is replacing investment in qualitative methods which would acknowledge the child's actual voice. Not only does data scraped from children's devices have economic benefits, as stated by Stoilova et al. (2021) above, but it is cheaper than conducting qualitative research with child participants which is labour-, time- and resource-heavy, and thus comparatively expensive. As a result, increasing children's agency over these datasets, including possible subversion of sensors collecting data, could encourage a return to qualitative methods which empower children's voices. Indeed, this was an initial motivation for this study. The methodology used to achieve this is outlined next.

STUDY DESIGN

The study sought to actively address issues of privacy and control arising from the increased use of sensors that collect user data embedded in digital devices commonly used by children. The original aims of the study were to understand what children already knew about sensors, to share ideas for subverting and blocking the sensors in their device, to gauge their interest in this and then, if they are interested, produce their own design and model paper prototypes for the purpose. The intention of the latter was that we would gain further insight into their thoughts on data collecting sensors through these methods whilst also empowering children aged 8–12 years by understanding

and, if they wanted, resisting/subverting embedded digital sensors. The aim was that in turn this might provide children with agency over how their lives are presented through data, and how this is used to inform a range of products aimed at making money from them. In relation to these points, the study used a mixed methods approach including a large number of visual methods. These are described next in relation to the two research questions they were used to address.

Methodology

This small-scale project involved 12 children aged 8–12 years. Each child joined one of four groups, and each group focused on exploring the research aims in relation to one of four types of digital device: an Amazon Alexa smart speaker, a smart watch, a smart phone, or a Nintendo Switch games console. These four devices were chosen because they are most commonly used by children (Ofcom, 2019); also, because they contain a wide range of sensor types (cameras, infrared depth, light, biometric, magnetometer, etc.) they would thus produce wider ranging data. The child participants were recruited via a professional recruitment company, such as those that are typical in market research. The recruitment company was asked to recruit four groups of three friends, with every participant in the group having access to the digital device that their group would focus on. Participants were organized into friendship groups to help them feel comfortable meeting two unknown adult researchers and maximize the chances of discussion between the research participants to enrich the dataset.

Following the recruitment, we met with each participant group twice for about 40 minutes each time, with a week's gap in between the first and second meetings. Due to COVID-19 restrictions, both sets of meetings took place via the video conferencing platform Zoom. In the first session, children were introduced to the research topic and took part in two activities (see Appendix 1) to explore their existing knowledge and attitudes towards sensors. Firstly, each child participant listed devices they knew contained sensors, the ways in which these could sense them, whether they thought that data was shared and, if so, who with. The second activity used drawing as a visual approach to data collection (e.g. Mayaba and Wood, 2015). Each participant drew around their device, and then depicted what they thought was inside. The child participants were free to use their imagination if they didn't know what something looked like. The intention was that these activities and accompanying conversations would engage participants at a distance, while also answering the first research question:

> *What do children understand about the sensing capabilities of digital devices they use?*

The second research session (see Appendix 2) used art and design-based methods and asked the child participants to use physical craft materials (which were posted to their homes in advance) to design tools to either block or trick the sensors in their devices into collecting inaccurate data. This was designed to address the second research question:

> How does the knowledge and use of creating sensor-disabling tools affect children's attitude towards digital sensing?

This drew on established practices from design methodologies called 'cultural probes' (Gaver et al., 1999; Wyeth and Diercke, 2006). Cultural probes typically involve a physical provocation or prompt to instigate design processes. In the case of our study, we designed physical provocations to be used in three steps. Firstly, participants were shown photographs of the inside of the devices revealing the sensors that we had asked them to speculate about in the first session. Secondly, they drew ideas for either blocking or tricking the sensors revealed in the first step. Thirdly, child participants modelled their inventions using the craft materials sent to them. In the second and third steps, children were told that their designs and models need not be practical. This is a speculative design concept which makes design a cognitive rather than a practical application (Dunne and Raby, 2013; Wargo and Alvarado, 2020). Speculative design was seen as particularly important for this project because the focus was on children's intentions and ideas rather than their skills to make working applications.

Ethical issues

In addition to applying for institutional ethical approval and adopting the best ethical guidelines for working with children set out by the British Educational Research Association (BERA, 2018), the methods were also considered part of decisions for ethical best practice. The methods drew from our experience of those used in both social sciences and art and design, and linked with our strong belief that methods are an important way of addressing the fact that it is a fundamental right of children to be included in research and have their voices heard (United Nations, 1989); further, that respect can be shown towards child research participants by studying areas relevant to their lives, showing genuine interest in their ideas and using a means of data collection that is appropriate and interesting. Further, involving children in research about surveillance and resistance responded to a desire to inform children about less ethical/unethical processes of data collection that they may not have been aware of.

Means of analysis

The mixed methods described above generated three types of data: (1) drawings, (2) models made from craft materials, and (3) video recordings of the group activities and accompanying conversations. The latter were recorded

via an in-built mechanism on the online video-conferencing platform, which children were informed of up front with verbal consent to use this function received from each child and parent. Each data type was analysed using individual means before the findings were compared across datasets. Specifically, video recordings were reduced to a voice-to-text audio transcript produced by the video-conferencing software. However, because voice-to-text transcription software is not fully accurate (especially in relation to children's voices), we watched all video data and corrected inaccuracies. We then applied Braun and Clark's (2006) approach to thematic analysis to produce a series of inductive and deductive themes.

Drawings were analysed using visual content analysis that produces a series of categories and quantifies the number of times these appear in the image dataset (Bell, 2001); for example, the number of times children had drawn wires. As with thematic analysis of the video data, this allowed us to understand which themes re-occurred in children's drawings most frequently. Finally, children's models were documented photographically (Figure 1), because they were produced at a distance, from which the software *Sketch-up* was used to render digital 3D images of the designs (Figure 2) in order to bring the 3D dimension into the analysis more easily. Comics were also drawn based on children's verbal descriptions of their models' functionality (Figure 3). Combining these means enabled us to use the Van Mechelen (2016) design framework to analyse the children's models. Essentially this uses methods of drawing out key themes in a similar vein to visual content analysis, but with a specific focus on 'listing design features' (Van Mechelen, 2016: 41). So, for example, one of the common design features was the use of pets.

Once the three different datasets had been analysed in these ways, the findings were compared for commonalities. In doing so, four broad themes emerged: (1) the role of inference in sensor awareness; (2) misunderstanding of device components and sensing capabilities; (3) attitudes to surveillance; and (4) subverting rather than blocking senses. These are discussed next.

FINDINGS AND DISCUSSION

Throughout the findings section, pseudonyms are used to represent the children in relation to the device their group focused on. So, 'N' represents the Nintendo Switch group, 'P' the phone, 'W' refers to smart watches and 'S' to smart speakers. The numbers after are used to distinguish between individual participants in the same group.

The role of inference in sensor awareness

Generally, the child participants showed good awareness of the existence of sensors in common digital devices, particularly phones/tablets, speakers, televisions and smart watches, which correspond to those most commonly accessed by children their age (Ofcom, 2019). When prompted further to

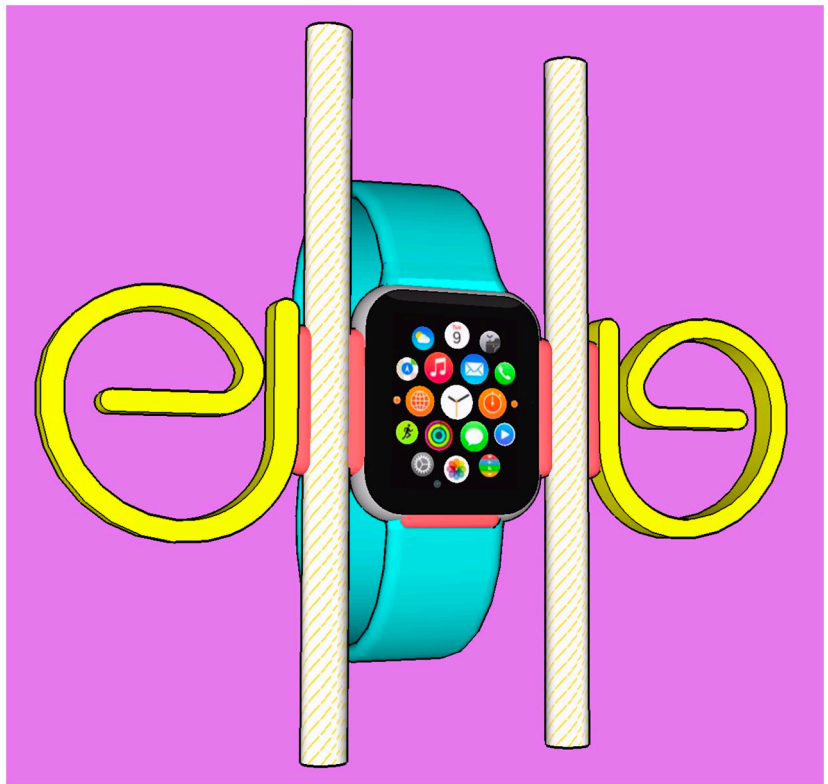**Figure 1.** A model of a sensor-blocking device for smart watches.

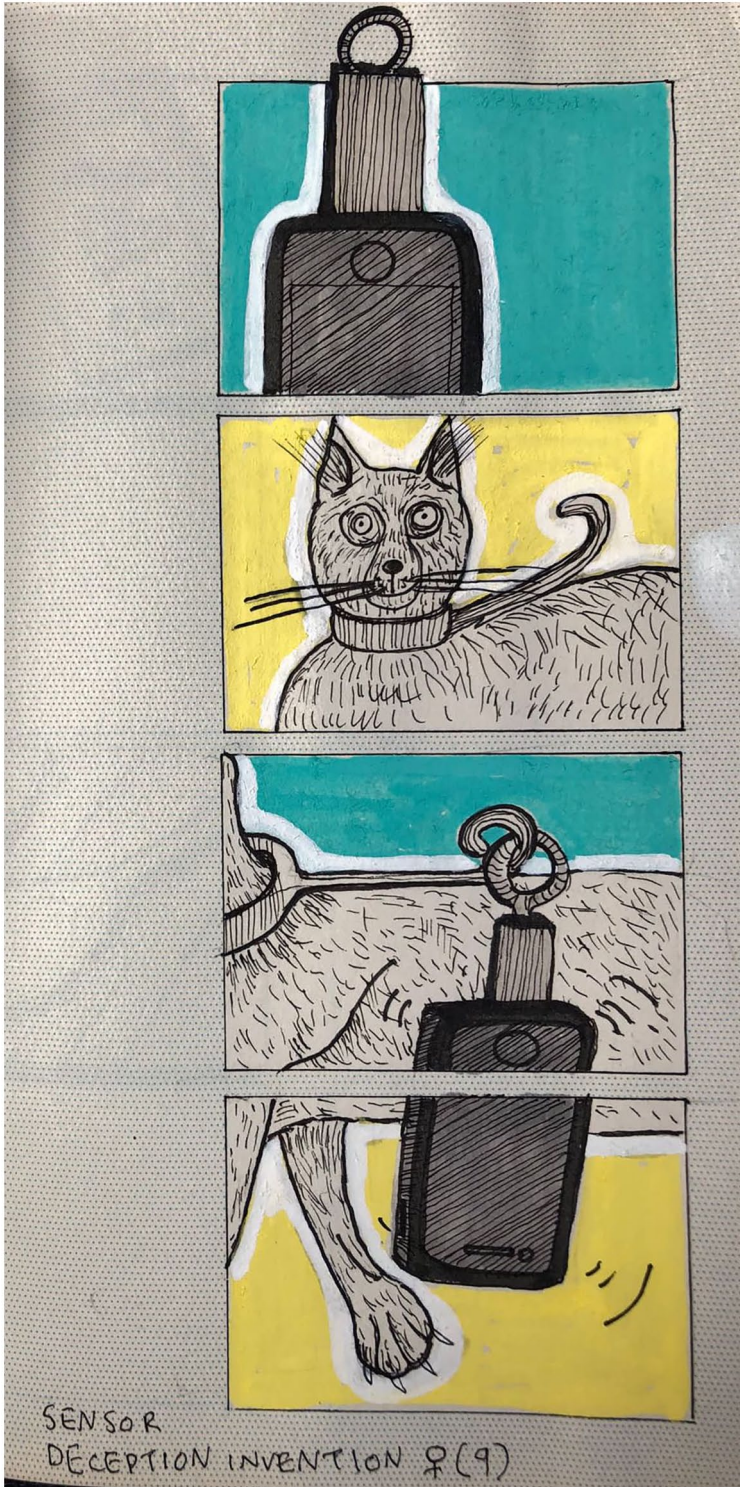**Figure 2.** A 3D render by Main (author) of the same object.

Figure 3. Comic transcription by Yamada-Rice (author) of a child's description of the functionality of their sensor deceiving model.

consider devices in relation to all household rooms, additional devices, such as games consoles, laptops, smart doorbells, smart lights, virtual reality headsets and cars, were also mentioned as containing sensors. Shrinking knowledge spiralling outwards from spaces most familiar to children to those less well known relates to other work about childhood knowledge such as Kenner's (2000) in relation to literacy practices.

Overall, children were aware of many sensors in their devices, but there were notable blind spots. In particular, sensor awareness corresponded with how much of a feature is made of the sensor in relation to device functionality. For example, face detection and fingerprint sensors were most commonly mentioned in relation to smartphones and identified by their trademarked names – FaceID and TouchID. Indeed, these trademarked names are prominent in advertising offering the market distinction of the device and thus have become household names. Further, these particular sensors are evident from the device's functionality. Thus, there is a clear link between cause and effect, helping children understand some of what the sensor detects and when. So, on an iPhone, placing a finger on a button, or showing a face to the screen, causes the pin number to be entered and the phone to unlock. Although it might be difficult to explain exactly how these sensors work, their presence and purpose are clear, and there is little ambiguity about the cause – scanning face/fingerprint and the effect identification.

The link between understanding and a clear cause and effect process occurred in children's discussions in relation to different devices and sensors, even with those we had not anticipated, such as cars. Several children described how cars contained sensors. Car sensors often perform safety functions and, as a result, the link between user behaviour and response is communicated clearly. The participants shared several anecdotes about their firsthand experience thus:

Researcher:	What do you think your car can sense about you?
W2 (female, 11):	If your seatbelt's clicked in.
W3 (female, 10):	If the door is open or not. If you're driving with the doors open this noise comes on.
W2:	It can sense what's in what seat, and what seat you're in.
P3 (female, 9):	Once I told my brother to get in the car, I had the car keys, and I tell him to get in but I shut the door and then I locked it, and he started moving around and the alarm went off.

The immediacy of these sensor feedback loops meant that children talked with certainty about what cars can sense about passengers. Similarly, where a sensing ability was a prominent or novel feature of a device, such as voice sensing for smart speakers, or heart rate for smart watches, then the children were able to readily identify the sensors. Relatedly, where sensors were less prominent,

children were not as aware of their use. For example, no child identified that smart watches contained microphones; instead, the participants named more prominent health sensors. Further, most participants overlooked cameras and GPS sensors on phones and tablets, with these longstanding features being overshadowed by more advanced, and therefore by Clarke's (1968) definition more 'magical', face and fingerprint sensors. As described in the literature review, this echoes the principles of misdirection that magic is heightened by; the constant development and marketing of new sensor features on devices means that attention can always be directed towards these, while others go unnoticed by users – something we believe device manufacturers use to their advantage.

Similarly, principles of misdirection can also be theorized in relation to children's perceived functionality of sensors used for extensive data inference. In relation to this, several children were aware that phone and watch sensors counted footsteps, but there is no specific 'footstep sensor' on these devices, as children believed. Instead, the step number is inferred using data from complex motion sensors like accelerometers and gyroscopes that children were not knowledgeable about. This is problematic because these same motion sensors can detect details of movement and environment that can be used to gain information about gestures, posture and physical habits. However, because step-counting is a prominent feature on watches and phones, and often visually displayed on the interface or used in apps, it is understandable that children would consider this the limit of their sensing abilities. Giving prominence to relatable, and fairly innocuous, features in this way can act to distract a user's attention from more subtle acts of sensing that are also happening. In other words, even the simplest form of data gathered from a sensor, such as steps, does not reveal the extensive anlaysis that can be further performed on the same data. Indeed the exact same data can be used to monitor sleep, study and meal times, etc. All participants in the study were surprised when we discussed this kind of information.

Just as digital devices are gaining information about children through inference, so the child participants were using inference to gain insights about the capabilities of their devices. In addition to the comments about cars, the child participants correctly inferred details about how their devices work by observing responses to specific actions:

N3 (male, 12):   [Discussing the lights on the side of the Nintendo Switch Joy-Con controller] The flashing lights they'll begin to flash when you take them off, so it senses that it's detached from the Switch, yeah.

W2 (female, 11):   [Discussing ways of tricking a smart watch into thinking you're walking]: I think it might need some heat on it to make it work, so if I had a light bulb or something I'd probably put that on to make it seem like it was our skin, because . . . it doesn't work when it's not on [my wrist].

Notably, it was the older participants aged 11 and 12 years who used their observations of the physical properties of the device to theorize its workings. The next section describes common misunderstandings in relation to sensors.

Misunderstanding of device components and sensing capabilities

Mistaken inferences led to fantastical thinking about the sensing abilities of devices and contributed to several misunderstandings children held about technology. Several children confused data captured from a sensor with data that is manually inputted, for example, believing a smart watch could use sensors to know a user's height:

P1 (female, 9):   [The Apple Watch] senses your height. My brother's apple watch knows how tall he is.

Other user-inputted data which children incorrectly thought was obtained by sensors included understanding their favourite colour, phone number, passwords and bank details. Maybe some of these misconceptions occurred because children are not responsible for inputting this kind of data and therefore assumed it arrived on the device via sensors. In the case of user data such as passwords, it seems likely that the children were conflating the idea of the device 'sensing' information with the device 'knowing' information. However, for some data it is possible that partial knowledge of the abilities of sensors leads to a magical impression of what's possible – after all, if a device can detect your face and your heartbeat, why not your favourite colour?

Further sensor misunderstanding stemmed from the networked nature of digital devices. Frictionless connection between different devices is often described in product descriptions as 'magical':

> AirTag features the same magical setup experience as AirPods – just bring AirTag close to the iPhone and it will connect. (Apple, 2021a, nd)

This kind of data flow can obscure the source of information during normal use by making it hard to understand if it is gained via sensors in the smart watch or the phone it is connected to:

Researcher: What else can [a smart phone] sense?
P1 (female, 9):   If there's a health app then sometimes it can feel your pulse, and it knows how fast your heart is beating, sometimes if it's super fancy.

In fact, phones don't have biometric sensors to detect heartbeat. This information arrives on a phone via the pulse sensor on a smart watch or fitness
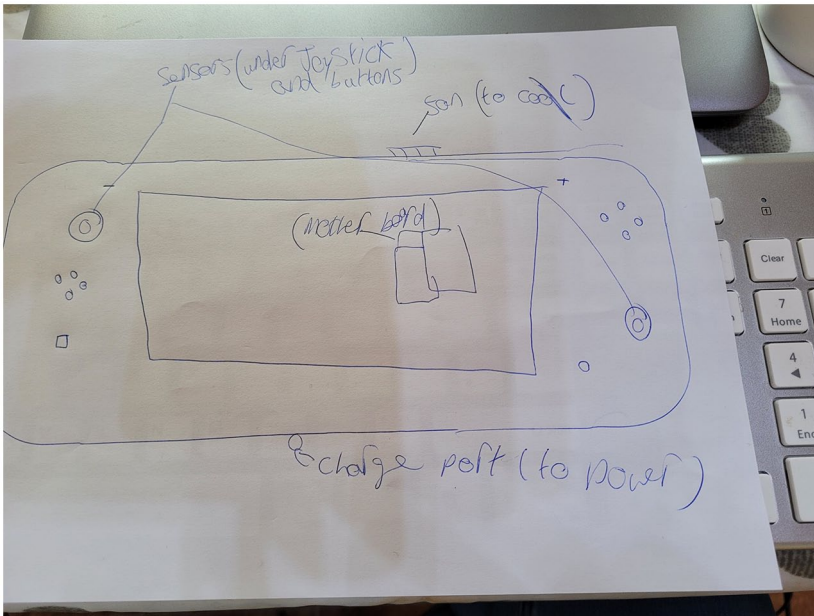
Figure 4. Inside a Nintendo Switch (N1, male, 11).

wearable. However, because the data is often made visible on phone inter-
faces, the confusion is understandable.

The analysis of child participants' drawings of the components inside
their devices also revealed opportunities for further education. Only two of
the older children (11 years old) attempted to draw a literal layout of device
components (Figures 4 and 5) and used external features of the device (but-
tons, ports, fan covers, etc.) to help speculate and locate the components
within the device.

The components most drew have a physical or visual presence on
the device exterior making them easily evident, i.e. cameras, microphones
and buttons. This kind of knowledge construction relates closely to Papert's
(1980) theory of 'body knowledge' which he uses to describe the importance
of observing physical mechanisms in order to understand connected 'abstract
and sensory' principles. In Papert's example, he explains how the presence of
cogs on a bicycle make it easy to understand how the vehicle works. Similarly,
information collected via a sensor attached to a visual/physical component
appears easier to understand how it works because its existence is evident.
Such ideas also link to the theories of material affordance (e.g. Gibson, 1979;
Norman, 2013) that show the extent to which humans can infer the uses of
different materials and objects through direct observation of their physical
properties. By comparison, digital materials, as we have shown, have many
invisible affordances. Thus, without the intuitive 'body knowledge' of cause
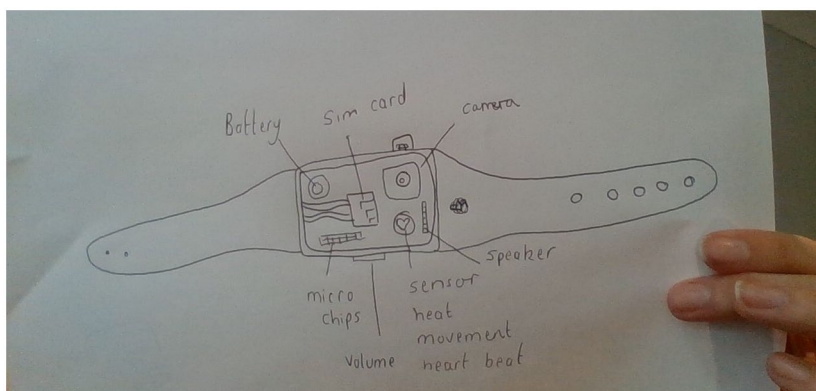and effect between physical actions, there is potentially less opportunity for
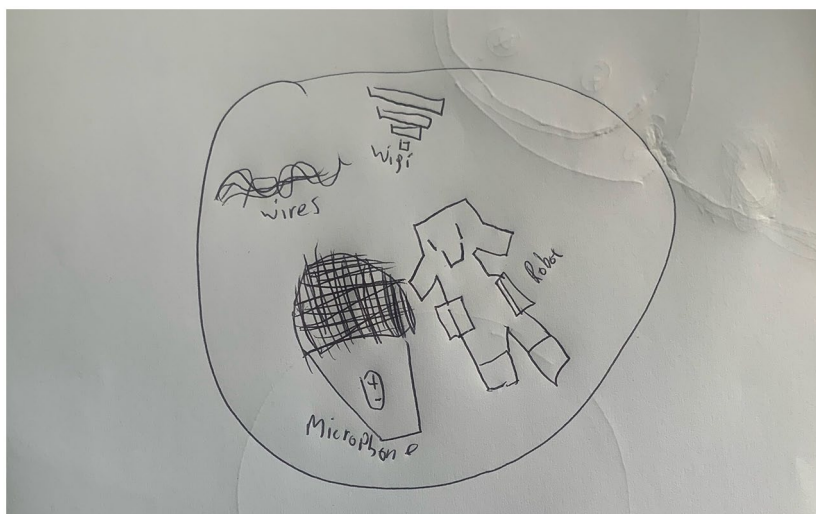
Figure 5. Inside a smart watch (W2, female, 11).

Figure 6. Inside a smart speaker (S1, male, 9).

children to gain a realistic understanding of the workings and capabilities of their digital devices, and more chance of imaginary explanations prevailing.

Similarly, children rarely considered internal items that could not be seen from the outside such as batteries or motion sensors. Additionally, the participants often used abstract symbols to represent components, rather than attempting literal representations reflecting how the chances to look inside a digital device are few. For example, children's drawings of cameras, microphones, pulse sensors, and wifi, were all based on icons used in device applications (Figure 6):

The prominence of wires in nearly all the drawings (see, e.g., Figures 7 and 8) was noteworthy because it reinforced a slightly old-fashioned analogue
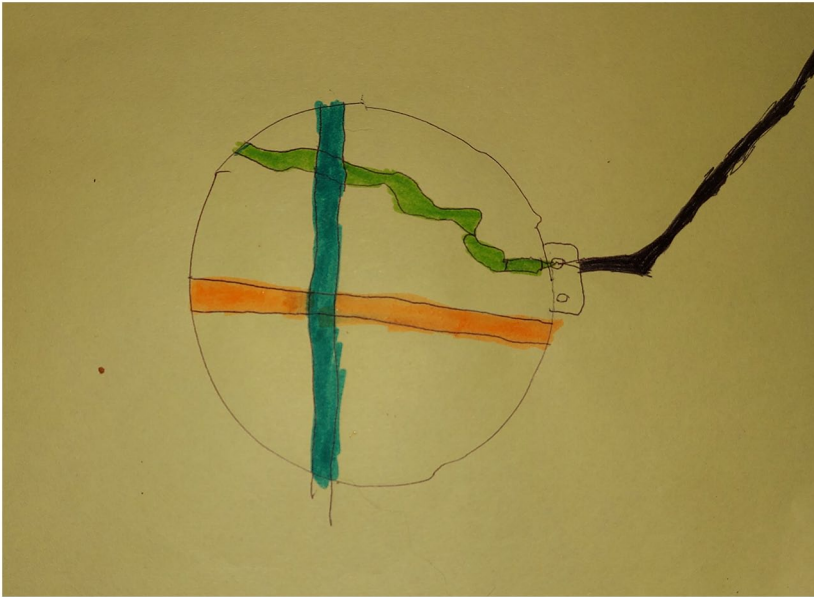
Figure 7. Inside a smart speaker (S3, male, 9).

impression of technology expressed by some of the children. Wires are rare in modern digital devices, having been replaced by printed circuit boards. Children appeared to be familiar with wires from images of older technologies that still regularly appear in children's books and even contemporary digital games such as *Assemble with Care* (Ustwo Games).

Such an interpretation also fits with the data that showed that when children were shown photographs of the inside of digital devices, they sometimes used older technology and media as a reference to describe what they saw:

P2 (male, 9): [Pointing to a wireless charging component] Is that a CD?

P1 (female 9): I think this CD looking thing. I think it might be something.

P2 (male, 9): [Referring to a camera component] It looks like a cassette tape, it looks like a tape.

As well as CDs and cassettes, children repeatedly misidentified components as batteries or SIM cards. It appears anachronistic that these older forms of technology are a reference point for young children; however, it is notable that such technologies are all objects that make visible connections between the internal and external device spaces, by requiring users to open them and insert or remove items from the internal workings. Like Papert's (1980) example of gears as physical objects which allow children to understand more complex concepts and relationships of how a bicycle works, these older analogue
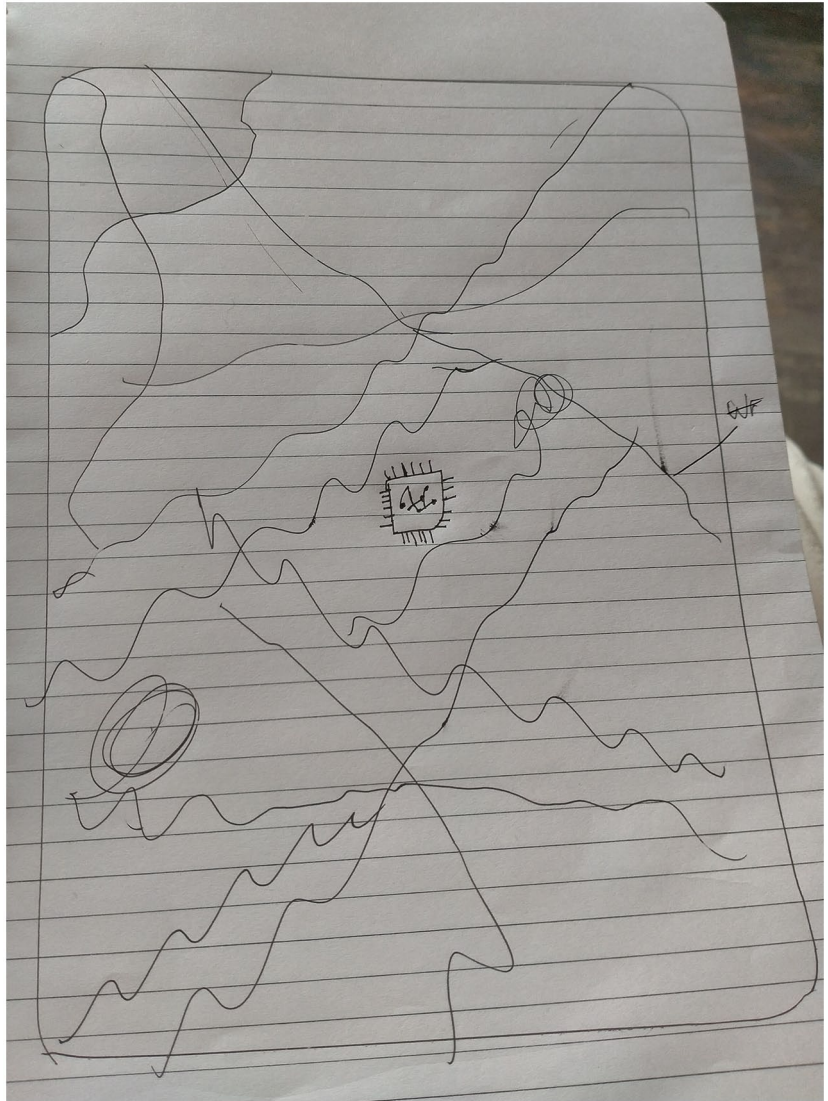
Figure 8. Inside a tablet (P2, male, 9).

technologies also contain physical working parts which can be examined and explored to reveal something about the nature of the system. Yet, such visible systems with tangible objects are much rarer in the age of streamed media and in-built batteries.

Generally, children understood that digital devices contained sensors but there were some blind spots. For example, games consoles and their controllers were frequently claimed not to sense people, despite the fact that game play often relies on the devices being able to precisely sense the movements of the player:

P2 (male, 9):	The Playstation doesn't really sense. It doesn't really sense you, sometimes it can, sometimes it can't . . . Wait, a controller senses a Playstation.
Researcher:	But do they sense anything about you?
P2 (male, 9):	No, not really.

Only half the participants mentioned laptops as containing sensors, and then only webcams and microphones (which they were actively using to attend the research sessions). There was some limited awareness of smart devices such as video doorbells and smart lighting, but the lack of prominence here might be due to the newness of such products and the ambient nature of their use.

We were interested in how the children had gained their existing knowledge about digital device components, and asked if they had ever been taught about their workings in school, or seen photographs, games, or videos anywhere. No one had. However, they all expressed interest in seeing inside their devices and learning more about how they worked, suggesting this might be a topic adopted in formal education settings.

As a work around, on several occasions when the child participants didn't know the answer to our question about what was inside, they used the device in question to search for information:

| P3 (female, 9): | [Typing on phone] I'm going on Google to check. |

We noticed that, in some cases, accurate responses to their questions were prevented:

S2 (male, 9):	Alexa, what's inside you?
Alexa:	Inside You is the 20th album by the Isley Brothers, and it was released on T-Neck Records on December 1st, 1981.
S2 (male, 9):	. . . Alexa, how are you made?
Alexa:	A lot of hard work from a lot of smart people.

This last lighthearted response by Alexa had a particular impact with the child in question, who was amused by the response. Although they used Alexa as a way of finding out practical information about how it worked, the playful response (such as those listed in Table 1) actually steered them towards a more fantastical idea. For the remainder of the focus group discussion, this child kept returning to the idea that their smart speaker literally contained 'smart people' and they wrote 'made of smart people' on their drawing of the inside of their smart speaker.

Attitudes to surveillance

The data analysis also highlighted how children's knowledge and misconceptions about digital sensing played into their broader attitudes to surveillance.

Insights in this area emerged from conversations about how they used their devices, and direct questions to ascertain their attitudes to overt surveillance systems such as CCTV. In the first research sessions, the children had predominantly positive attitudes towards public surveillance. This is likely connected, as Birnhack et al. (2018: 204) point out, to the fact that children of this age will have 'been born and raised in a digital world with its ubiquitous surveillance'. However, unlike in Birnhack et al.'s study where the Israeli primary school children 'value their privacy and are willing to relinquish it only when they perceive it as justified' (p. 204), the children in this study were uncritical of it. When asked whether they thought CCTV in their school was good or bad, all participant groups replied in a vein similar to this:

Researcher:	What do you think about [CCTV in school]? Is that a good thing or a bad thing, or have you never thought about it?
W1 (female, 10):	It's a good thing.
W2 (female, 11):	It's a good thing, makes you safe.
Researcher:	How does it keep you safe?
W2 (female, 11):	Watching. It's watching if like people are trying to come in, or trying to do something bad. It's also if someone gets told off and then it's a really bad thing you can check the cameras to see if it actually happened and see who's lying.

The positive perception of CCTV as an arbiter of truth in school situations was repeated by several others. For example:

N2 (male, 12):	[CCTV in school] is good because, like some kids, well naughty kids, they kicked down this bin, and if a teacher walks by and seen this bin on the floor, they can say we've got CCTV so we can check who did it.
N1 (male, 11):	Someone told one of teachers that someone else was coughing in their face. The head of the year, she went down to CCTV area and she found who did it, and he actually got expelled.

The predominant attitude expressed by children was that, in schools, CCTV surveillance was omniscient and benign, always present to resolve disputes and catch 'naughty kids'. When asked if there were any spaces that should not be covered by CCTV, they were only concerned about personal spaces like bathrooms. This links with the work of Rooney (2010) that shows how surveillance in some contexts, particularly with children, has been conveyed as a form of care, which Barron (2014) links to the way in which surveillance apps and technology have been sold to parents as a means of keeping their children safe.

N3 (male, 12):   Around my school . . . there's like CCTV like every-where. Obviously not in the bathroom because that's just illegal.

Reservations about surveillance in private spaces was limited to visual surveillance and based on a concern about being seen, rather than heard or sensed in other ways.

Researcher: What about things that can hear you or things which can sense when you're moving? Are there any times you don't want them hearing you or sensing when you're moving?

S2 (male, 9):   No.

Our initial intention for the study design with the research workshops was to co-design anti-surveillance tools with children, as a way of determining what methods and approaches would best provide children with agency over surveillance by digital devices. However, through the first stage of the research sessions, it became clear that, as the children's attitude to surveillance was predominantly positive and their knowledge of sensors often limited, the bigger challenge of the research became understanding how to better inform them about digital sensing and engage them in issues of surveillance. As a result, it is not surprising that children's ideas about surveillance by sensors began to change. In particular, this emerged during the second workshops in producing speculative design models to either block or subvert sensors from collecting data about them. The children's designs revealed further insights about their attitudes to digital sensing. These are described next.

Subverting rather than blocking sensors

Barron's (2014: 4) research found that children in the same age group as the ones we worked with 'clearly demonstrate the ability to negotiate with their parents in relation to the monitoring of their everyday lives'. Similarly, our data showed how children expressed more interest in 'negotiating' being monitored by sensors, through selectively disrupting observation or feeding them false information, than fully blocking the sensors. We invited the child participants to create an invention that would block or trick one of the sensors on their devices. Because they had expressed positivity about surveillance and therefore were possibly not particularly predisposed to imagine contexts for anti-surveillance tools, we decided to provide them with some specific scenarios. For the group using phones/tablets and smart watches, this was to think about health apps and ways of tricking the motion sensor into believing they were exercising when they weren't. For the smart speaker group, they focused on ways they could say 'Alexa' in front of the device without being heard and waking it. Whereas, the Nintendo Switch group downloaded a free

Figure 9. A device to attach a phone to a cat to increase step count.

game, Jump Rope Challenge, and invented a means of deceiving the game into believing they were jumping.

The findings showed that the majority of children chose to design tools which tricked, rather than disabled, the sensors on their devices. Rather than remove or disable the sensor, one girl aged 10 designed a mechanism for attaching her mobile phone to a cat to increase her step count (Figure 9):

Other children used movement created by inanimate objects to trick the sensor in the same way; a 9-year-old girl designed a device to swing the phone and increase her step count (Figure 10):

Figure 10. An invention to swing a smart phone.

Or for creating the illusion of skipping to be picked up by sensors in the Nintendo Switch when they were not skipping (Figure 11).

These examples link with the work of Barron (2014: 401) that illustrated how 'children in middle childhood negotiate and resist the monitoring and surveillance of their physical selves in time and space using mobile phones predominantly.' However, it is notable that the children in this study did not appear to do this naturally, rather it came as a response to our demonstrating what sensors were capable of, and providing prompts in the form of a cultural probe made of craft materials. Perhaps one reason children appeared interested in subverting rather than disabling sensors was that they were keen (even in
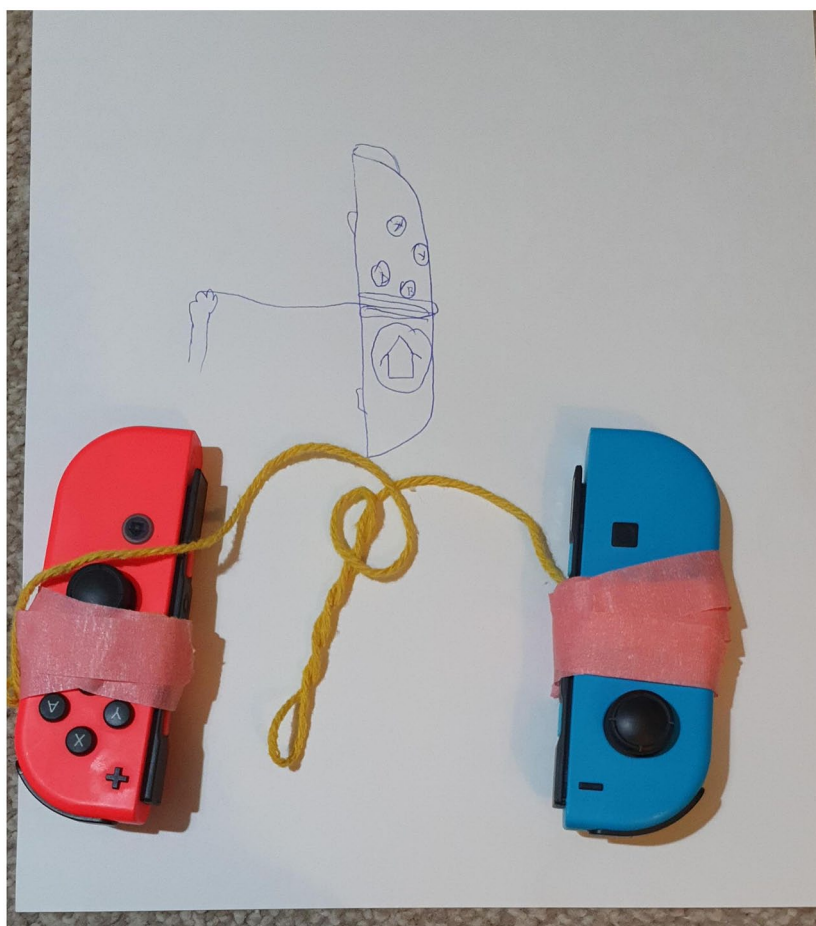
Figure 11. A device for swinging the Nintendo Switch controllers.

a hypothetical sense) to ensure their devices were not irreparably affected by their speculative models and made inventions that could be applied or removed from devices when desired, which reiterates the importance of digital devices to children (Ofcom, 2019).

Finally, children's designs demonstrated how they were capable of reversing the power dynamic between technology companies using misdirection with data collecting sensors in their own designs. This can be understood by returning to the model for attaching a phone to a cat (Figure 9). In making this model, the child inferred (incorrectly) that a heat sensor was activated as part of the step counting and that the temperature of the cat would allow this to continue working.

REFLECTIONS AND CONCLUSIONS

The concluding findings were that children's knowledge of digital sensors was often limited, and incorrect influences were usually made when the cause and

effect of sensors were invisible. Relatedly the greatest awareness of sensors was in relation to those that were highly visible and regularly used, such as the camera. Additionally, awareness increased when sensors formed part of an immediate feedback loop, such as when a child uses biometric data, like a finger print or facial recognition to unlock their phone. It follows then that learning about secondary information that could be retrieved from the sensors was mostly new to the children in this study. Connected to this was that children's general awareness of being surveilled was largely in relation to the data being linked to known humans, for example knowing a teacher might look at CCTV footage at school, or that their parent is interested to see their step count on their phone. What appeared unknown is how secondary information collected by sensors is used. Stoilova et al. (2021) write of the general tension that this data, which forms a massive part of the 'data economy', brings about between commercial organisations and those that worry for children's privacy and wellbeing. Specifically, they state 'policy makers often hope that more media literacy education can solve the problem, fearing that new regulation could impede digital innovation' (p. 558). Based on the findings of this study, we also advocate for media education. Specifically, given the successful way in which the child participants responded to the hands-on and visual methods that formed our methodology, we believe in the power of media education that allows children to explore the otherwise invisible inside workings of digital devices, as well as being offered opportunities to break, disrupt and block sensors as a way of gaining knowledge through their hands – what Ingold (2013) refers to as knowing through doing. This links with work undertaken by other researchers working in the areas of emerging tech and children. For example, Robertson et al. (2017: 339) write that children's understanding 'that computer software carries out instructions via a processor that laboriously reads a long string of 0s and 1s builds awareness that computers are not capable of magically performing intelligent feats'.

Likewise, work by Yamada-Rice et al. (2019) shows how, when children were taught to build working cardboard virtual reality headsets, they came to understand the rational processes of how 2D images become 3D, and were thus able to better critique the technology and the content it uses. In relation to this, the findings of this study offer suggestions for areas that could be explored further.

Children were keen to see what was inside their devices and learn more about how they worked, suggesting more work could be done to explore how the long-held genre of cross-sectional drawings, 'what's inside' models or take apart puzzles could be extended with digital, not just analogue materials. Resources which explain what is inside devices, and how they work, could be popular with children and create more awareness about surveillance and privacy strategies. Applications, such as games, which provide direct, concrete feedback about what a device is sensing could help establish correct causal associations and create better awareness of surveillance. Such games exist with

analogue technologies such as ustwo Games's Assemble with Care but we were unable to locate anything similar for newer digital tech.

Others, such as Gross and Eisenberg (2007) and Tanimoto (2004) have argued for transparency and realism in the design of objects for children, rather than the ambiguity of magical metaphors. We agree with this argument for better communication of the methods and capabilities of digital devices, particularly in relation to the consequences of sensing and surveillance. However, we also believe that such approaches do not necessarily need to be traded-off between magical experiences and transparency. Given the enthusiasm expressed by the children in our study towards seeing inside devices and learning how they work, it seems that one central principle of magic may not apply in this context – children can enjoy the magical effects afforded by technology whilst also observing the methods that created them. Knowing how the trick is done does not necessarily spoil the experience. Likewise, devices could provide more information themselves about how they work and what their sensing capabilities are. This is particularly relevant to smart speakers and voice assistants.

Finally, we are also happy to note that this month the UK Information Commissioner's development of a code of practice for age-appropriate design also forces changes to the commercial side of data collection in relation to these sensors too. It is now no longer acceptable for companies to collect information that is deemed unnecessary for the task being carried out by the child user. Holding organizations to account in this way, while also providing children with greater media literacy in relation to the sensors and their works, provides a two-pronged approach to the many issues at stake in children's lives being surveilled by tech companies and more.

ORCID ID

Dylan Yamada-Rice https://orcid.org/0000-0002-3917-9197

REFERENCES

Apple (2007) Apple reinvents the phone with iPhone. *Apple News Room*. Available at: https://www.apple.com/uk/newsroom/2007/01/09Apple-Reinvents-the-Phone-with-iPhone (accessed 17 September 2021).

Apple (2016) Apple reinvents the wireless headphone with AirPods. *Apple News Room*. Available at: https://www.apple.com/uk/newsroom/2016/09/07Apple-Reinvents-the-Wireless-Headphone-with-AirPods (accessed 17 September 2021).

Apple (2018) HomePod arrives February 9, available to order this Friday. *Apple News Room*. Available at: https://www.apple.com/uk/newsroom/2018/01/homepod-arrives-february-9-available-to-order-this-friday (accessed 17 September 2021).

Apple (2019a) All-new iPad Air and iPad mini deliver dramatic power and capability. *Apple News Room*. Available online at: https://www.apple.com/uk/newsroom/2019/03/all-new-ipad-air-and-ipad-mini-deliver-dramatic-power-and-capability (accessed 17 September 2021).

Apple (2019b) Apple reveals new AirPods Pro, available October 30. *Apple News Room*. Available at: https://www.apple.com/uk/newsroom/2019/10/apple-reveals-new-airpods-pro-available-october-30 (accessed 17 September 2021).

Apple (2021a) Apple introduces AirTag. *Apple News Room*. Available at: https://www.apple.com/uk/newsroom/2021/04/apple-introduces-airtag/ (accessed 17 September 2021).

Apple 2021b) Clips adds immersive new AR Spaces. *Apple News Room*. Available at: https://www.apple.com/uk/newsroom/2021/04/clips-adds-immersive-new-arspaces (accessed 17 September 2021).

Barron CM (2014) 'I had no credit to ring you back': Children's strategies of negotiation and resistance to parental surveillance via mobile phones. *Surveillance & Society* 12(3): 401–413.

Bell P (2001) Content analysis of visual images. In: Van Leeuwen T, Jewitt C (eds) *Handbook of Visual Analysis*. London: Sage, 10–34.

BERA (2018) Best ethical guidelines for working with children. Available at: https://www.bera.ac.uk/publication/ethical-guidelines-for-educational-research-2018-online (accessed 18 October 2021).

Birnhack M, Perry-Hazan L and German Ben-Hayun S (2018) CCTV surveillance in primary schools: Normalisation, resistance, and children's privacy consciousness. *Oxford Review of Education* 44(2): 204–220.

Braun V and Clark V (2006) Using thematic analysis in psychology. *Qualitative Research in Psychology* 3(2): 77–10.

Clarke AC (1968) Clarke's Third Law on UFOs. In: Wigner EP, Time and Effort Reports Defended. *Science* 159(3912): 255.

Day M, Turner G and Drozdiak N (2019) Is anyone listening to you on Alexa: A global team reviews audio. Bloomberg.com. April 2019:N.PAG. Available at: https://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=140638783&authtype=shib&site=ehost-live (accessed 13 October 2021).

Dunne A and Raby F (2013) *Speculative Everything: Design, Fiction and Social Dreaming*. Cambridge, MA: MIT Press.

Frazer JG (1996) *The Golden Bough: A Study in Magic and Religion*. London: Penguin.

Gaver B, Dunne T and Pacenti E (1999) Cultural probes. *Interactions* 6(1), January/February: 21–29.

Gibson JJ (1979) *The Ecological Approach to Visual Perception*. Boston, MA: Houghton, Mifflin and Company.

Green N (2002) Who's watching whom? Monitoring and accountability in mobile relations. In: Brown B et al. (eds) *Wireless World: Social, Cultural and Interactional Issues in Mobile Technologies*. London: Springer.

Gross MD and Eisenberg M (2007) Why toys shouldn't work 'like magic': Children's technology and the values of construction and control. *First IEEE International Workshop on Digital Game and Intelligent Toy Enhanced Learning (DIGITEL'07)*, IEEE, 25–32.

Hyman R (1981) 'Cold reading': How to convince strangers that you know all about them. *Zetetic* 1(2): 18–37.

Ingold T (2013) *Making: Anthropology, Archaeology, Art and Architecture*. London: Routledge.

Kenner C (2000) *Home Pages: Literacy Links for Bilingual Children*. Stoke-on-Trent, UK: Trentham Books Limited.

Kuhn G (2019) *Experiencing the Impossible: The Science of Magic*. London: The MIT Press.

Kuhn G, Caffaratti H, Teszka R and Rensink R (2014) A psychologically-based taxonomy of misdirection. *Frontiers in Psychology*, 5.

Lamont P and Wiseman R (1999) *Magic in Theory: An Introduction to the Theoretical and Psychological Elements of Conjuring*. University of Hertfordshire Press.

Marquardt P et al. (2011) (sp)iphone: Decoding vibrations from nearby keyboards using mobile phone accelerometers. In: *Proceedings of the 18th ACM Conference on Computer and Communications Security*, Chicago, IL, 17–21 October, 551–562.

Mayaba NN and Wood L (2015) Using drawings and collages as data generation methods with children: Definitely not child's play. *International Journal of Qualitative Methods* 14(5): 1–10.

Michalevsky Y, Boneh D and Nakibly G (2014) Gyrophone: Recognizing speech from gyroscope signals. In: *23rd {USENIX} Security Symposium* 14: 1053–1067.

Norman D (2013) *The Design of Everyday Things*, rev. and expanded edn. New York, NY: Basic Books.

Ofcom (2019) Children and parents: Media use and attitudes report. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf (accessed 13 March 2022).

Papert S (1980) Preface: The gears of my childhood. In: *Mindstorms: Children, Computers, and Powerful Ideas*. New York, NY: Basic Books.

Piaget J (1929) *The Child's Conception of the World. Translated by J & A Tomlinson*. London: Routledge & Keegan Paul.

Ring Blog (2021) Available at: https://blog.ring.com/neighborhood-stories/how-to-help-kids-be-safe-engaged-and-connected-this-school-year/; home cameras: available at: https://en-uk.ring.com/products/mini-indoor-security-camera (accessed 13 March 2022).

Robertson J, Manches A and Pain H (2017) 'It's like a giant brain with a keyboard': Children's understandings about how computers work. *Childhood Education* 93(4): 338–345.

Rooney T (2010) Trusting children: How do surveillance technologies alter a child's experience of trust, risk and responsibility? *Surveillance & Society* 7(3/4): 344–355.

Rosengren KS and French JA (2013) Magical thinking. In: Taylor M (ed.) *The Oxford Handbook of the Development of Imagination*. Oxford: Oxford University Press, 42–60.

Stoilova M, Nandagir R and Livingstone S (2021) Children's understanding of personal data and privacy online: A systematic evidence mapping. *Information, Communication & Society* 24(4): 557–575.

Tanimoto S (2004) Transparent interfaces: Model and methods. In: *Proceedings of the AVI Workshop on Invisible and Transparent Interfaces, Gallipoli, Italy*. New York, NY: ACM.

Tapper J (2020) Alexa, Siri . . . Elsa? Children drive boom in smart speakers. *The Guardian*, 18 October. Available at: https://www.theguardian.com/technology/2020/oct/18/alexa-siri-elsa-children-drive-boom-in-smart-speakers (accessed 10 September 2021).

UK Information Commissioner's Office (2020) Age-appropriate design: A code of practice for online services. Available at: https://ico.org.uk/media/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf (accessed 4 February 2022).

United Nations (1989) Convention on the Rights of the Child. Available at: https://www.unicef.org.uk/what-we-do/un-convention-child-rights (accessed 13 March 2022).

Van Mechelen M (2016) Designing technologies for and with children: A tool kit to prepare and conduct co-design activities and analyse the outcomes. *Mint Lab*. DOI: 10.1007/978-3-030-10898-4_9.

Wargo JM and Alvarado J (2020) Making as worlding: Young children composing change through speculative design. *Literacy* 54: 13–21.

Wyeth P and Diercke C (2006) Designing cultural probes for children. *Proceedings of the 18th Australia conference on Computer-Human Interaction: Design: Activities, Artefacts and Environments*, November: 385–388.

Yamada-Rice D, Rodrigues D and Zubrycka J (2019) Makerspaces and virtual reality. In: Blum-Ross A et al. (eds) *Enhancing Digital Literacy and Creativity: Makerspaces in the Early Years*. London: Routledge.

Zuboff S (2019) *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power*. London: Profile Books

BIOGRAPHICAL NOTES

ANGUS MAIN is a Tutor in Information Experience Design at the Royal College of Art. He has a MRes in Information Environments from London College of Communication and is currently studying for a PhD at the University of the Arts London, Creative Computing Institute, researching how AI can be used to support creativity. His research focuses on the impact of emerging technologies on experiential communication. Main was most recently PI on an EPSRC-funded project called 'Countermeasures' which investigates how to increase children's awareness of sensor-based surveillance, using co-design and ethnographic research methods with children aged 8–12 years. Before this, he was a Co-I on the AHRC-funded Japan-UK VR project, exploring how Physical Computing and tangible interfaces contribute to location-based VR experiences. *Address*: Royal College of Art, London, UK. [email: angus.main@rca.ac.uk]

DYLAN YAMADA-RICE is a Senior Lecturer in Immersive Storytelling in the School of Digital Arts, MMU. She is an artist and researcher specializing in storytelling and play, and works in a range of media including drawing, film photography and Virtual Reality. Dylan studied Japanese Art History, Semiotics and Social Science research methods before moving into Experimental Design. This interdisciplinary background has brought about a specialism in the role of culture in storytelling and use of emerging technologies, as well as how art and design practices can be combined with Social Science research methods to produce experimental means of collecting and analysing data. She has previously held academic posts at the University of Sheffield and in Information Experience Design at the Royal College of Art. *Address*: Manchester Met University, All Saints, Manchester M15 6BH, UK. [email: d.yamada-rice@mmu.ac.uk]

Appendix 1. Workshop 1 plan and field questions.

5 mins	Introduction – housekeeping Dylan	• Ask about recording • Let them know how they can opt out of questions/activities at any stage
15 mins	Breadth of sensing technology they have access to. *List-making task*	• Think of all the electronic devices in your house. Can you write down as many as possible which can **sense** you in some way (for example, which ones can hear you, see you, or sense when you're moving)? • What kind of things can they sense? • Which ones are connected to the internet?
10 mins	What's inside your device? *Drawing task*	• Thinking about the specific devices you have with you today. On a piece of paper, draw an outline of your device (you can draw around the device itself if that's easier) • Inside that outline draw what you think is inside your device. Don't worry if you don't know what it looks like in there. You can use your imagination as much as you want. • Show your pictures to the webcam when you're finished.
5 mins	Who sees the data? *Open discussion*	• Does anyone see the information that your device senses about you? If so, who?
5 mins	Wrap up	• For next week, think about the parts of your device which do the sensing. Where are the microphones/cameras/motion sensors etc. and how could you stop them sensing you?

Appendix 2. Workshop 2 plan and field questions.

Sensor follow-up discussion 10 mins	*Discussion*	• How does your device sense movement/sound? • How would you know what was inside a device? • [Show image inside device] • Have you ever taken anything apart? • What do you think the components are?
Fooling sensors 10 mins	*Discussion*	• Did you think of any ways you could fool your device? • [Show examples from tool kit] • If you could build a tool which helped you fool your device, or stop it sensing you, what would it do?
Draw a tool 10 mins	*Drawing*	• Can you draw a picture of a tool which would help you fool your device or stop it sensing you? • It doesn't have to work. You can use your imagination.
Making challenge 20 mins	*Making*	• Using the materials provided, can you make a model of your tool?
Demonstrate outcomes 10 mins	*Discussion*	• Show the models that have been made, and describe/demonstrate how they would work • Capture images using the webcam and ask for other photos to be emailed
Wrap up 10 mins	*Discussion*	• Would you use a tool like this? • What would you use it for? • How do you feel about the sensors on your device?