The Rise of the Algorithmic Child: Protecting Children in Smart Homes

Victoria Nash

We usually think of children's contact with the Internet through the lens of popular entertainment activities such as scrolling through social media, playing games, or watching videos, typically undertaken on personal devices. While these activities shape our perception of children's online engagement, especially because their enjoyment is visible and their usage easily measurable, these are not the only ways in which children interact with online services. In fact, there are at least three key ways in which children now routinely engage with digital service providers online[1]:

1. Actively, and most frequently consciously, via digital apps, services, or content on their own devices, or devices shared with other family members;
2. Passively or unconsciously via screenless devices employed around the home;

[1] This typology expands on a distinction drawn by the UK Children's Commissioner. Cf. UK Children's Commissioner: Who knows what about me?

This research summary draws on findings from a project funded by the Oak Foundation (OCAY-16-667): Child Safety on the Internet: Looking Beyond ICT Actors. I am very grateful to Dr. Huw C. Davies and Dr. Allison Mishkin for their research assistance on this project.

V. Nash (✉)
Oxford Internet Institute, University of Oxford, Oxford, UK
e-mail: victoria.nash@oii.ox.ac.uk

N. Dethloff et al. (eds.), *Families and New Media*, Juridicum – Schriften zum Medien-, Informations- und Datenrecht,
https://doi.org/10.1007/978-3-658-39664-0_10

3. Actively or passively via services set up by third parties and used outside of the home, such as educational tools or services in schools, or on public WiFi networks.

The first of these is well documented in survey-based literature, which provides solid evidence-based research that details which activities are most popular with different age groups across countries, as well as which risks and opportunities children face in their daily use.

The third might seem an unfamiliar focus, but in the years before personal mobile devices became ubiquitous, political battles were fought over how best to keep children safe from adult content when using computers in public spaces such as libraries or schools. In the United States, for example, early efforts to introduce federal-level legislation to protect minors from indecent or offensive communications resulted in the Children's Internet Protection Act (2000) which established compulsory Internet filtering for schools and libraries in receipt of public funding. In the current context of ubiquitous mobile access, attention to welfare in the digital public realm has turned instead to the possible risks associated with connecting personal devices to public WiFi networks, not just in libraries or schools, but in shops, cafes and public transport systems.[2] Similar concerns about access to harmful content have played out on this stage too, resulting in the provision of services such as the United Kingdom's 'friendly' WiFi certification,[3] whereby public providers offer filtered Internet access that would prevent access to adult content such as pornography or illegal content such as child abuse imagery. Security and privacy concerns relating to children's use of public Internet services or networks have yet to receive significant policy attention, but the growing array of academic literature analysing possible risks of data-driven services in contexts such as education suggests this may yet change.[4]

Thus whilst active personal Internet use of devices and apps, and public use outside the home are familiar subjects for both research and policy-making, the second form of Internet access is less well-understood, limiting the potential for providing appropriate safety guidance or policy oversight. It is this topic that forms the basis of the discussion that follows.

[2] Cf. Spacey et al.: Filtering Wireless (WiFi) Internet Access in Public Places, Journal of Librarianship and Information Science 49 (1), 2017, pp. 15–25.

[3] Cf. Friendly Wifi: Website.

[4] Cf. Hakimi/Eynon/Murphy: The ethics of digital trace data in education, Review of Educational Research 91(5), 2021, pp. 671–717.

First we need to clarify what we mean by passive or unconscious interaction with screenless devices around the home. The focus on devices without screens is deliberate, as this both alters the mode of interaction (no text, images or videos) and also occludes the digital connectivity of the device—smart devices don't look like familiar phones or computers, potentially making it harder for both adults and children to 'read' their capabilities or risks. Similarly, the focus on passive or unconscious use is also important. Whereas children, even young toddlers can quickly become aware of the enjoyment brought by direct engagement with simple games or videos on a phone or a tablet device, many of the screenless devices in focus here are either a hidden part of the digital landscape of the home and family life or are disguised as analogue toys, with additional functionality potentially hidden from view. Both of these factors make it more challenging for users to understand the digital risks and opportunities of engaging with such devices.

To further clarify these points, it is worth specifying the types of product or service that would fall into this category. Children now have access to a range of Internet-connected devices at home that extend beyond the familiar screen-based smartphones, tablets, or computers, to include many of the following:

- Connected or smart toys that use Internet connectivity to provide interactive features such as the ability to respond to a child's questions or touch[5];
- Smart home assistants, such as Amazon's Alexa or Google Home, which provide a voice-based interface connected directly to the Internet, enabling users to access an array of functions such as playing music, ordering products, providing information or even telling jokes, simply by voicing a command[6];
- Surveillance or tracking technologies, such as smartwatches, that enable parents to monitor their child's location or Internet-connected cameras to remotely monitor babies, children, or childcare workers whilst parents are away from the house[7]; and
- 'Babytech' products that include quasi-medical devices, such as smart socks, to measure heartrate and blood oxygenation, as well as fertility trackers or Bluetooth enabled products like nappies or baby bottles that notify parents when to intervene.[8]

[5] Cf. Holloway/Green: The Internet of toys, Communication Research and Practice, 2(4), 2016, pp. 506–519; Chaudron et al.: Kaleidoscope on the Internet of Toys.

[6] Cf. Mascheroni: Datafied childhoods, Current Sociology, 68(6), 2020, pp. 798–813.

[7] Cf. Mascheroni: Datafied childhoods, Current Sociology, 68(6), 2020, pp. 798–813.

[8] Cf. Leaver: Intimate surveillance, Social Media + Society, 3(2), 2017, pp. 1–10.

Although the products described above are nowhere nearly as ubiquitous as mobile phones or tablets, they are used by a significant number of children. For example, according to industry figures, 78 million smart home assistants were sold worldwide in 2018.[9] Almost 10% of children in the United Kingdom used smart home assistants such as Amazon Echo or Google Home to go online in 2018, and a similar rate was reported for the United States in 2017.[10] In terms of other devices, 8% of British children used Internet-connected toys, and 5% had used wearable devices like smartwatches.[11] In the United States, 15% of two to four year olds were reported to have a connected toy.[12]

So far, research shows little evidence of harm resulting from children's use of these new classes of digital devices. However, a closer look at news reports does reveal numerous instances of security flaws or data breaches. The My Friend Cayla doll was, for example, banned in Germany after the country's telecommunications regulator classified the toy as an 'illegal espionage apparatus' because of its reliance on an unsecured Bluetooth connection which enabled anyone within a certain range to listen in on conversations or even speak to the child through the doll.[13] The same regulator also banned the sale of children's smartwatches for similar reasons.[14] Cloudpets, a brand of stuffed animals, were removed from online stores like Amazon after it emerged that consumer voice recordings (including those of children) were stored in unsecured databases, had been accessed by unauthorized parties, and had even been used to hold people to ransom.[15] Other examples include the VTech data breach, during which servers containing customer information and children's personal data were hacked[16]; numerous incidents of baby monitors being hacked (and in some cases being used to speak to a child or broadcast video feeds on the Internet); and multiple reports from consumer organizations demonstrating security flaws in devices like smartwatches.[17]

[9] Cf. Canalys: Smart speaker market booms in 2018.

[10] Cf. Common Sense Media: The Common Sense Census.

[11] Cf. Livingstone/Blum-Ross/Zhang: What do parents think, and do, about their children's online privacy?

[12] Cf. Common Sense Media: The Common Sense Census.

[13] Cf. Oltermann: German parents told to destroy doll that can spy on children.

[14] Cf. Wakefield: Germany bans children's smartwatches.

[15] Cf. BBC: Children's messages in CloudPets data breach.

[16] Cf. Gibbs: Toy firm VTech hack exposes private data of parents and children.

[17] Cf. Laughlin: Kids' smartwatches vulnerable to hackers; Forbrukerrådet: #WatchOut.

Such reports are undoubtedly concerning, but do they really have implications for child welfare, and do they necessitate a new policy response? Security weaknesses in smart home devices may in turn provide easy access to all other devices on a network, including devices that record images or conversations inside homes, as well as store personal data, videos, photos, and passwords. Once accessed, such data can be sold on the dark web, used to buy goods and services, empty bank accounts, or extort.[18] Sadly, such cyber-crimes are not uncommon; however, as of now, there is little evidence that security weaknesses or data theft have resulted in direct harm to children.

There is rather a more insidious and less tangible type of risk conceptualized in the literature analyzing the societal implications of the data economy: the way that data about children is used to make decisions about their lives.[19] Children's data is increasingly being captured and transmitted by the array of new connected devices appearing in many homes, often without much awareness by parents. This data may be utilized to generate reports, recommendations, or notifications about children as part of the service that is offered. For example, 'baby tech' devices, such as smart baby socks or mattresses, use data including motion, temperature, and even heartrate monitors, to analyze a child's wellbeing and inform parents or caregivers of any concerning changes. While tracking devices let parents know exactly where their children are, they may also offer more detailed analysis that enables them to understand more about their children's play habits or even friendships.

The use of these technological aids is undoubtedly well-intended, but the data generated gives the illusion of objectivity and neutrality while at the same time representing only the aspects of a child's life that a company has chosen to record. These digital glimpses of a child's life are described as 'data assemblages', reflecting the fact that they are assembled from parts of a person's life or behavior as viewed through the lens of a particular technology.[20] The risk that results from such 'data assemblages' is that they come to substitute more holistic, personal, and situated knowledge of a child.[21] Parents using smart baby

[18] See, for example, BBC: Miss Teen USA hacker jailed for 18 months.

[19] Cf. Lupton/Williamson: The datafied child, New Media & Society, 19(5), 2017, pp. 780–794.

[20] Cf. Lupton: How do data come to matter?, Big Data & Society, July-December 2018, pp. 1–11.

[21] Cf. Lupton/Williamson: The datafied child, New Media & Society, 19(5), 2017, pp. 780–794.

technologies may privilege the information provided by those technologies rather than trust their own parental judgement about their children; a teacher or school may base important decisions affecting children's educational welfare on the data gathered through a specific online tool rather than on the harder-to-quantify messier realities of children's lives. In many cases, we might hope that using such technologies would improve our decision-making. The risk, though, is that it comes to replace decision-making, in the sense of active consideration of children's best interests. Further, it reduces children's lives to just a series of ones and zeros while making adults feel as if they are better, more responsible caregivers.

The appeal of such technologies is evident. Exhortations that a monitored child is a safe child abound in advertising and marketing strategies that offer parents "Peace of Mind Through Every Milestone",[22] or make claims about "Revolutionising the cot so you can sleep too".[23] But there are more concrete risks to a growing reliance on childcare technologies, especially if it means abandoning our own better judgement. Many of the new 'baby tech' devices and apps are marketed as providing health data that you would expect to be provided only by regulated healthcare devices. Yet the reality is that few of these new technologies are well-regulated, meaning there is no guarantee that the devices will provide accurate, reliable information. There have yet to be tragedies resulting from inaccurate readings, or failed alerts, but paediatricians have provided explicit warnings about the risks to consumers and their families.[24] Similar concerns have been raised about the legitimacy of decisions made in education that are based on app-generated data.[25] Ultimately, these technologies create what could be called 'an algorithmic child', and the risk is that in trying to satisfy the needs and wellbeing of this partial, datafied 'algorithmic child', we ignore the child's actual individual and self-claimed needs.

How might such risks be mitigated? Across Europe, children's welfare and interests are protected by many different regulatory instruments, at both the national and supranational levels. In the context of the types of product discussed in this chapter, the most significant regulatory frameworks relate to toy safety, data

[22] Owlet: Website.

[23] smart cot: Website.

[24] Cf. Bonafide/Jamison/Foglia: The Emerging Market of Smartphone-Integrated Infant Physiologic Monitors, JAMA., 317(4), 2017, pp. 353–354.

[25] Cf. Jarke/Breiter: Editorial: the datafication of education, Learning, Media and Technology, 44(1), 2019, pp. 1–6.

protection, and consumer protection. However, these leave some obvious gaps in the regulatory framework for children's use of connected devices in the home. Security standards for Internet of Things (IoT) devices have yet to be agreed upon at the international level, and it remains unclear how agreements would be enforced in terms of keeping insecure products away from consumers. Consumer protection laws are largely provided by European Union Member States—and enforced with varying degrees of enthusiasm. Internet safety for children is currently largely governed by self-regulatory measures and has thus far focused primarily on content and contact risks. Individual European Union Member States have national legal frameworks to cover criminal conduct and content, such as child sexual abuse, imagery, or grooming, whilst initiatives to develop media literacy and build resilience amongst young Internet users also receive varying levels of investment in different countries. There are some examples of more wide-ranging measures being introduced which recognise the need for a more holistic approach to regulating online risks and harms. Beyond Europe, Australia passed a Digital Safety Act in 2021,[26] whilst in the United Kingdom, an Online Safety Bill has been published and seems likely to become law in 2022/23. This Bill establishes a wide-ranging regulatory framework targeting a variety of online harms, and vitally, imposes a new 'duty of care' on technology companies to prevent these, particularly in relation to children, albeit still with a focus predominantly on content.[27]

None of these approaches seems adequate in the face of the privacy and security-related risks outlined above. Data protection frameworks instead seem to offer the most obvious protection, and indeed the European Union's General Data Protection Regulation (GDPR) awards children special protection in virtue of their more limited ability to understand the implications of personal data processing for their rights and interests.[28] However, as Lievens and Verdoodt note, there are several points on which even the GDPR fails to provide sufficient clarity in relation to the processing of children's data, including whether direct marketing can constitute a legitimate ground for processing children's data, and whether or not the GDPR provides enough protection against the use of children's data

[26] Cf: Minister for Communications, Urban Infrastructure, Cities and the Arts: Digital Safety Act.

[27] Cf. Minister for State for Digital and Culture: Draft Online Safety Act.

[28] Cf. Lievens/Verdoodt: Looking for needles in a haystack, Computer Law & Security Review, 34(2), 2018, pp. 269–278.

for the creation and use of profiles about them.[29] Neither of these gaps causes problems uniquely for children's engagement with the types of product or service discussed in this article, but rather demonstrate that further clarification is needed from data protection authorities in order to provide full protection for children.[30]

One interesting initiative, which may better protect children's data and privacy interests from devices in the smart home, is the United Kingdom's Age-Appropriate Design Code. Introduced as a result of an amendment to the United Kingdom's Data Protection Act, it is intended to ensure that all companies providing information society services (ISS) "likely to be accessed by children" act in children's best interests in data collection and processing, offering a set of fifteen basic standards to guide such action.[31] These standards require, for example, that such companies maintain high privacy standards by default, map the data gathered from UK children, check the ages of users to ensure appropriate protections are offered, avoid using 'nudge' techniques to encourage children to provide more personal data and switch off geolocation services by default. The types of companies listed include those providing apps, websites, search functions, social media and online messaging, but explicit mention is also made of the types of service discussed here: "Electronic services for controlling connected toys and other connected devices are also ISS."[32]

The Code was implemented in 2020 and companies were given a transitional year in which to adapt to the requirements. As enforcement thus only began in September 2021 it is still too early to ascertain how impactful this Code will prove to be. Remarkably though, and coinciding with the end of the transitional period, Facebook, Instagram, Tik-Tok, Google and YouTube all announced the introduction of changes to their services which purport to offer strengthened privacy protections for younger users. None cited the Code, and the changes will seemingly be global rather than solely UK-based, but as likely early targets for enforcement action, it seems plausible that implementation of the Code has prompted such moves.[33] Such early successes do not necessarily indicate that

[29] Cf. Lievens/Verdoodt: Looking for needles in a haystack, Computer Law & Security Review, 34(2), 2018, pp. 269–278.

[30] Cf. Milkaite/Lievens: The Internet of toys, in: Mascheroni/Holloway (eds.): The Internet of Toys 2019.

[31] Cf. Information Commissioner's Office: Age appropriate design: a code.

[32] Cf. Information Commissioner's Office: Age appropriate design: a code.

[33] Cf. Stokel-Smith: Britain tamed big tech and nobody noticed, Wired Magazine.

there will be widespread changes across the sector however, not least because it is well-understood that the body responsible for enforcing the Code, the UK's Information Commissioner's Office (ICO) lacks the resources to monitor or enforce compliance on a large scale. But complaints have already been filed against these and other big tech companies by children's rights organisations, meaning that it should soon become clear how effective the ICO will be in upholding UK children's privacy rights.

Is this enough? In an economic and technological environment where personal data is a source of private profit, the digital wellbeing of both adults and children are inescapably bound to the willingness of private companies to take their ethical and regulatory responsibilities seriously. To date, self-regulatory initiatives to protect children have largely focused on engaging big tech companies, seeing these stakeholders as the most significant players in the battle to keep children safe and happy online. But with the rise of smart devices, such as connected toys, digital home assistants, and 'baby tech', it is now clear that there is a long trail of companies, both big and small, who must take their responsibilities to protect young users (and their data) seriously. Against this backdrop, children's rights, the ethics of capturing and managing their data, and its potential for commercial exploitation are deservedly but belatedly beginning to receive more attention. We may not be able to challenge the fundamental business models that drive the dataveillance practices outlined above, but there is an urgent need for critical data research that can shed light on the extent and purpose of data collected from children in order to inform future policy-making and public debate. This symposium makes a vital contribution to that mission.

References

BBC: Children's messages in CloudPets data breach, BBC News, February 28, 2017, https://www.bbc.co.uk/news/technology-39115001; last accessed May 26, 2021.

BBC: Miss Teen USA hacker jailed for 18 months, BBC News, March 18, 2014, https://www.bbc.co.uk/news/technology-26616913; last accessed May 26, 2021.

Bonafide, Christopher P./Jamison, David T./Foglia, Elizabeth E.: The Emerging Market of Smartphone-Integrated Infant Physiologic Monitors, JAMA., 317(4), 2017, pp. 353–354.

Canalys: Smart speaker market booms in 2018, driven by Google, Alibaba and Xiaomi, 2019, https://www.canalys.com/newsroom/smart-speaker-market-booms-in-2018-driven-by-google-alibaba-and-xiaomi; last accessed May 26, 2021.

Chaudron, Stéphane/Di Gioia, Rosanna/Gemo, Monica/Holloway, Donell/Marsh, Jackie/Mascheroni, Giovanna/Peter, Jochen/Yamada-Rice, Dylan: Kaleidoscope on the

Internet of Toys—Safety, security, privacy and societal insights, JRC (Joint Research Centre) Technical Reports, Luxembourg 2017, JRC105061, EUR 28397 EN.
Common Sense Media: The Common Sense Census: Media Use by Kids Aged Zero to Eight, 2017, https://www.commonsensemedia.org/sites/default/files/uploads/research/csm_zerotoeight_fullreport_release_2.pdf; last accessed May 26, 2021.
Forbrukerrådet (Norwegian Consumer Council): #WatchOut. Analysis of smartwatches for children, 2017, https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf; last accessed May 26, 2021.
Friendly WiFi: Website, https://www.friendlywifi.com; last accessed November 2, 2021.
Gibbs, Samuel: Toy firm VTech hack exposes private data of parents and children, The Guardian, November 30, 2015, https://www.theguardian.com/technology/2015/nov/30/vtech-toys-hack-private-data-parents-children; last accessed May 26, 2021.
Hakimi, Laura/Eynon, Rebecca/Murphy, Victoria A.: The ethics of digital trace data in education: a thematic review of the research landscape, Review of Educational Research 91(5), 2021, pp. 671–717.
Holloway, Donell/Green, Lelia: The Internet of toys, Communication Research and Practice, 2(4), 2016, pp. 506–519.
Information Commissioner's Office: Age appropriate design: a code of practice for online services, 2020, https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf; last accessed October 19, 2021.
Jarke, Juliane/Breiter, Andreas: Editorial: the datafication of education, Learning, Media and Technology, 44(1), 2019, pp. 1–6.
Laughlin, Andrew: Kids' smartwatches vulnerable to hackers, Which?, October 18, 2017, https://www.which.co.uk/news/2017/10/kids-smartwatches-vulnerable-to-hackers/; last accessed May 26, 2021.
Leaver, Tama: Intimate surveillance: Normalizing parental monitoring and mediation of infants online, Social Media + Society, 3(2), 2017, pp. 1–10.
Lievens, Eva/Verdoodt, Valerie: Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation, Computer Law & Security Review: The International Journal of Technology Law and Practice, 34(2), 2018, pp. 269–278.
Livingstone, Sonia/Blum-Ross, Alicia/Zhang, Dongmiao: What do parents think, and do, about their children's online privacy? Parenting for a Digital Future: Survey Report 3, London 2018.
Lupton, Deborah: How do data come to matter? Living and becoming with personal data, Big Data & Society, July-December 2018, pp. 1–11.
Lupton, Deborah/Williamson, Ben: The datafied child: The dataveillance of children and implications for their rights, New Media & Society, 19(5), 2017, pp. 780–794.
Mascheroni, Giovanna: Datafied childhoods: Contextualising datafication in everyday life, Current Sociology, 68(6), 2020, pp. 798–813.
Milkaite, Ingrid/Lievens, Eva: The Internet of toys: playing games with children's data?, in: Mascheroni, Giovanna/Holloway, Donell (eds.): The Internet of Toys. Studies in Childhood and Youth, 2019.
Minister of Communications, Urban Infrastructure, Cities and the Arts: Online Safety Act (Cth), Australia, 2021, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p

;query=Id%3A%22legislation%2Fbillhome%2Fr6680%22; last accessed October 19, 2021.
Minister of State for Digital and Culture: Draft Online Safety Bill, https://www.gov.uk/government/publications/draft-online-safety-bill; last accessed November 2, 2021.
Oltermann, Philip: German parents told to destroy doll that can spy on children, The Guardian, February 17, 2017, https://www.theguardian.com/world/2017/feb/17/german-parents-told-to-destroy-my-friend-cayla-doll-spy-on-children; last accessed May 26, 2021.
Owlet: Website, https://owletbabycare.co.uk; last accessed October 19, 2021.
smart cot: Website, https://www.smart-cot.com; last accessed May 26, 2021.
Spacey, Rachel/Muir, Adrienne/Cooke, Louise/Creaser, Claire/Spezi, Valérie: Filtering wireless (Wi-Fi) Internet access in public places, Journal of Librarianship and Information Science, 49 (1), 2017, pp. 15–25.
Stokel-Smith, Chris: Britain tamed big tech and nobody noticed, Wired Magazine, September 2, 2021, https://www.wired.co.uk/article/age-appropriate-design-code-big-tech; last accessed October 19, 2021.
UK Children's Commissioner: Who knows what about me?, London 2018, https://www.childrenscommissioner.gov.uk/digital/who-knows-what-about-me/, last accessed December 2, 2022.
Wakefield, Jane: Germany bans children's smartwatches, BBC News, November 17, 2017, https://www.bbc.co.uk/news/technology-42030109; last accessed May 26, 2021.

Prof. Dr. Victoria Nash is Director of the Oxford Internet Institute (OII), UK, where she is also an Associate Professor and Senior Policy Fellow. Her research interests draw on her background as a political theorist, and concern the normative policy implications of evidence characterizing children's use of Internet technologies. She holds several digital policy advisory roles, including membership of the World Economic Forum Global Coalition for Digital Safety, the UK Government's multi-stakeholder UK Council on Internet Safety (UKCIS) Evidence Group, and serves on the Advisory Board of Internet Matters.