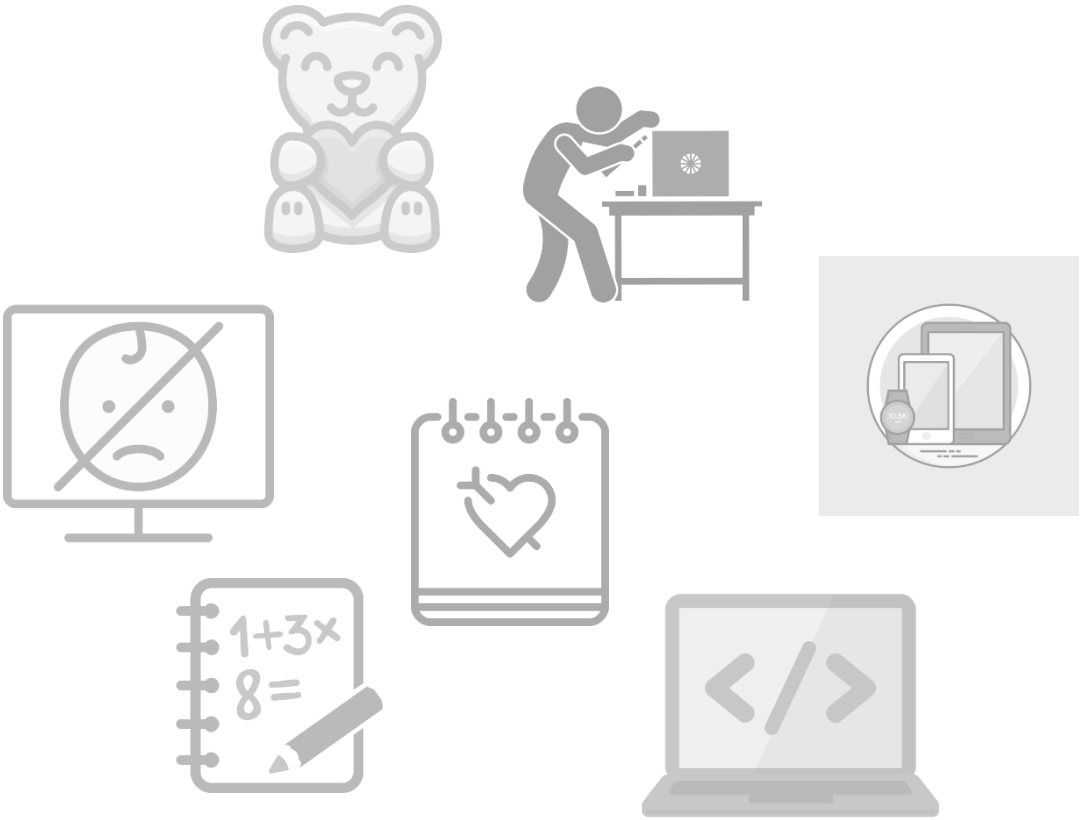


Connected Toys:

What Device Documentation Explains about Privacy and Security

White paper

Sarah Turner

DOI: 10.14324/000.rp.10100395

Executive Summary

This report looks at the amount of safety and privacy information that is publicly available about Internet connect devices that are targeted at children.[1] By reviewing the documentation and advertisements related to 15 prominently marketed devices for children it tries to determine how easy it is for the purchasers of the device to understand whether devices connect to the Internet, and if so, what security and privacy implications it has for carers and for the children themselves. It finds that it is uniformly hard to determine the nature of technology within any given device; where devices do connect to the Internet, no information is provided to users regarding privacy and security best practices, and how functional the device is without connection to the Internet. Similarly, there is limited explanation of the personal data that must be provided to make the device run as intended, and also of how to delete this information once the device is no longer in use. The report comes up with a number of considerations for carers who have children with connected devices, and recommendations for device manufacturers, to promote a more informed purchasing process, and a less risky environment for children's play and development.

Considerations for carers:

- Do I know how it connects to the internet? If the device connects to a home Wi-Fi network, am I happy with all the individuals who have the password to that network?
- Do I understand what personal data the device, and any associated software, uses in relation to my child? Where would it make sense to use fake data (such as nicknames)?
- Does my child understand what I can see of their data? Are they happy with how I use that data?
- Can I delete the child's data once the toy is no longer actively used?
- Can the child's data be moved to an adult account, should they be using the device once they hit the age of data processing consent? Do I know what the difference between the child and adult app is?

Recommendations for manufacturers:

- Clearly state on the packaging and in the manual where a toy requires connection to the Internet, and explain within the manual what functionality is lost should a toy not be connected.
- Point users to recognised cyber-hygiene and security guidance within the documentation.
- Do not require children's names or ages as part of the registration/account naming process; rather recommend the use of pseudonyms.
- Clearly state in the manual what data is collected about the child, how this is held, and for what purpose.
- Make the default option for selling or give a child's data to third parties, particularly for advertising purposes, opted out. Opting out of such data processing should not encroach on the functionality of the toy.
- Clearly explain the methods of removing all personal data from the device/relevant data storage mechanisms, coupled with a clearly available take out and deletion mechanism.[1] This should be instantaneous, and should not involve email or other personal contact with individuals or teams at the manufacturer.

[1]Throughout this report, "children" will be used to describe those who are below the age of data processing consent. For example, legislation in the United States (the Children's Online Privacy Protection Act, or "COPPA") determines this to be 13; in the European Union, this is captured as part of the General Data Protection Regulation ("GDPR"), but is determined by the Member State: the age range is currently between 13 and 16 years old in these countries.

Connected toys: an introduction

In a parallel to devices marketed at adults, there are an increasing number of toys that are equipped with sensors and actuators to automate interactions with users, connect to the Internet (primarily for the purpose of collecting, using or sharing data) or both (FPF/FOSI, 2016). The phenomenon of the "Internet of Toys" is not a new one to research or consumer awareness groups: as with other devices connected to the Internet, there are concerns over the security and privacy of both individual toys and the practices of entire manufacturers (Forbrukerradet, 2016; Coldeway, 2018). Compounding these concerns is the lack of a unified approach to explain to the consumer the types of security processes a manufacturer uses (for example, traffic-light labelling schemes (Blythe and Johnson, 2018)). There is also tacit understanding that individuals do not read the privacy policies that are used to explain how personal data is used (Obar and Oeldorf-Hirsch (2018)). Children in particular are ill-prepared to deal with inappropriate or unexpected uses of technology, and so the concerns about the potential for abusive use, when out of sight of the caregiver, has raised particular concerns (see, for example, Laughlin (2017)). Higher standards of security measures required by manufacturers would be a measure to allay some of the fears that research on current devices may raise (for children's devices in particular, see *inter alia*, Chu et al (2019)).

The current approach for managing children's use of digital products is parental consent. However, this is problematic, as the introduction of software and data collection has created a complexity in the relationship between child and toy: an adult now needs to take ongoing responsibility for agreeing to the terms of service of the device, and may need to provide additional devices (tablets, apps) for the toy to work at all (Mascheroni and Holloway, 2017). A toy is no longer something that is solely a child's to play with. It is clear from a reading of the General Data Protection Regulation ("GDPR"), however, that the regulatory intent is not that children are unaware of what happens with their data: indeed, Article 12(1) suggests that this information must be written in such a way that it is intelligible to the child (Ni Loidean, 2019). This requirement is in line with what children want: Coleman et al. (2017) found that children would welcome shorter, more understandable documentation, perhaps using audio or video as a means of putting the message across.

Recognising the issues that prior research has found in relation to connected devices aimed at children (henceforth "connected toys"), this report aims to produce recommendations for both carers and manufacturers. This is done by looking at products available for purchase in the run up to Christmas 2019,[2] and asking specific questions on the following themes:

- How easy is it to tell that a device must be connected to the Internet to work as intended?
- How easy is it to determine the security and privacy measures taken by the manufacturer?
- What does the adult responsible for agreeing to the terms and conditions have to do to make the device work as intended?

[2] The review was undertaken between 31 October and 10 November 2019

Methodology

Table 1	
Theme	**Specific questions posed**
How easy is it to tell that a device must be connected to the Internet to work as intended?	Is the product a connected device?
	Is the technology used within the device explained at all?
How easy is it to determine security and privacy measures taken by the manufacturer?	Are there reference to IoT device security or commonly accepted cyber hygiene practices in the product manual or the privacy policy?[3]
	Do any news articles relating to the manufacturer's inappropriate use of data, insecure systems or any other such negative press make it on to the first two pages of a Google news search?[4]
	Do the available privacy policies (on the website of the manufacturer) clearly explain the use of children's data?
	Is it explained on the website, manual or privacy policy how to delete personal data from the toy?
	What is the reading level of those privacy policies with explicitly aimed at children, or discussing children's data?
What does the adult responsible for agreeing to the terms and conditions have to do to make the device work as intended?	Does the product require the use of an app, website or other supportive technology (either software or hardware)?
	How do adverts market the product?
	If the product is marketed at children who may use the device over the age of consent for data processing, what guidance is given to the adult as to how to facilitate this change?

Table 1 explains the relationship between the themes outlined in the Introduction and the more detailed questions considered for every connected toy. The researcher answered these questions for each connected device with information that was freely available without buying the device. It was considered that this would be appropriate, as this is the type information that individuals have prior to purchasing such products (following, amongst others, Blythe et al., 2019).

This research and its findings are based on a systematic review of the publicly available documentation of 15 connected toys .[5] These 15 toys were found through taking the details of 200 listings on amazon.co.uk,[6] and from two articles from widely distributed UK newspapers aimed at adults considering buying such products for children.[7] Duplicate listings were only reviewed once, and those listings that were not related products (for example, SD memory cards, protective cases

[3] The types of security and practices considered here are those listed in "Code of Practice for consumer IoT security"(2018) as well as the National Cyber Security Centre's guidance pages "Smart Devices: using them safely in your home" (2109) and "Top tips for stay secure online" (2018)

[4] When the search terms "manufacturer" + "toy name", and then just "manufacturer" are used.

[5] These toys include those that connect to the Internet through a wired connection to a computer, and, in one case, a non-connected toy that is marketed alongside an app.

[6] Specifically, those products that were listed as the top 100 in the "Electronic Toys, 4 stars and up", and "Electronic Toys, Educational Computers and Accessories, 4 stars and up"

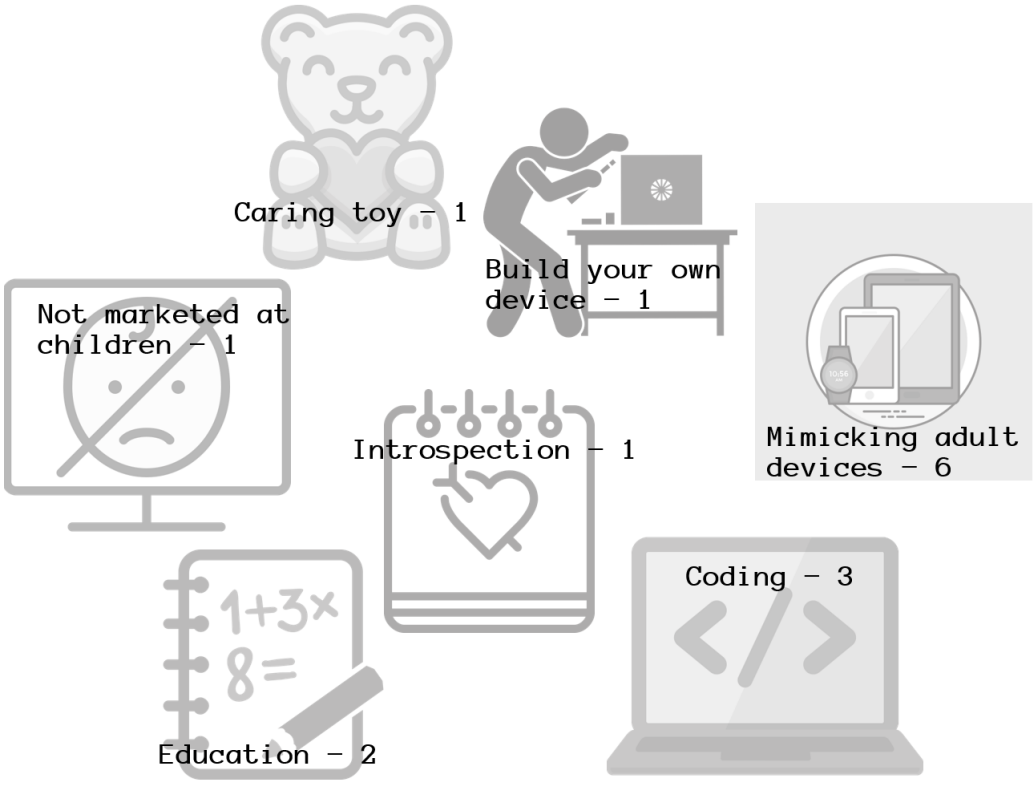
[7] Yeoman, 2017; Morris, 2019.

for tablets, books) were removed. This left an initial set of 56 products, of which 15 were in scope. Product listing, downloadable manuals, privacy policies and advertisements and news articles were subject to thematic review, using the questions in table 1 as a prompt.[8]

Results

How easy is it to tell that a device must be connected to the Internet to work as intended?

A key finding is how difficult it is to determine whether a product needs to be connected to the Internet to work as intended. The search categories used on amazon.co.uk – a website chosen expressly because of its market penetration[9] – were based on the "electronic toys" category, as it was the closest aligned segment that may include connected toys. This meant that those products that are connected and/or smart devices were listed alongside toys that had no such technologies – for example, toys with lights and motors, walkie-talkies, and toy microphones. Of the 56 products that were initially included for review, only 15 were connected toys, and they fell into the following categories:



Categories of devices reviewed

Whether products were connected to the Internet is not uniformly explained in the product marketing. Neither is, in the case of connected toys, how functional the toy might be without the connection to the Internet. In some cases – where products are used in conjunction with a connected device (such as Osmo), or are mimicking adult devices (such as the Garmin Vivofit Jr), it is perhaps not necessary to explain this. However, other products may not so obviously need a connection to the Internet, and the need for a connection is often only mentioned within the

[8] Full results of the review undertaken can be found here.

[9] See, for example, "Leading search engines ranked by market share UK 2019 | Statista", (2019)

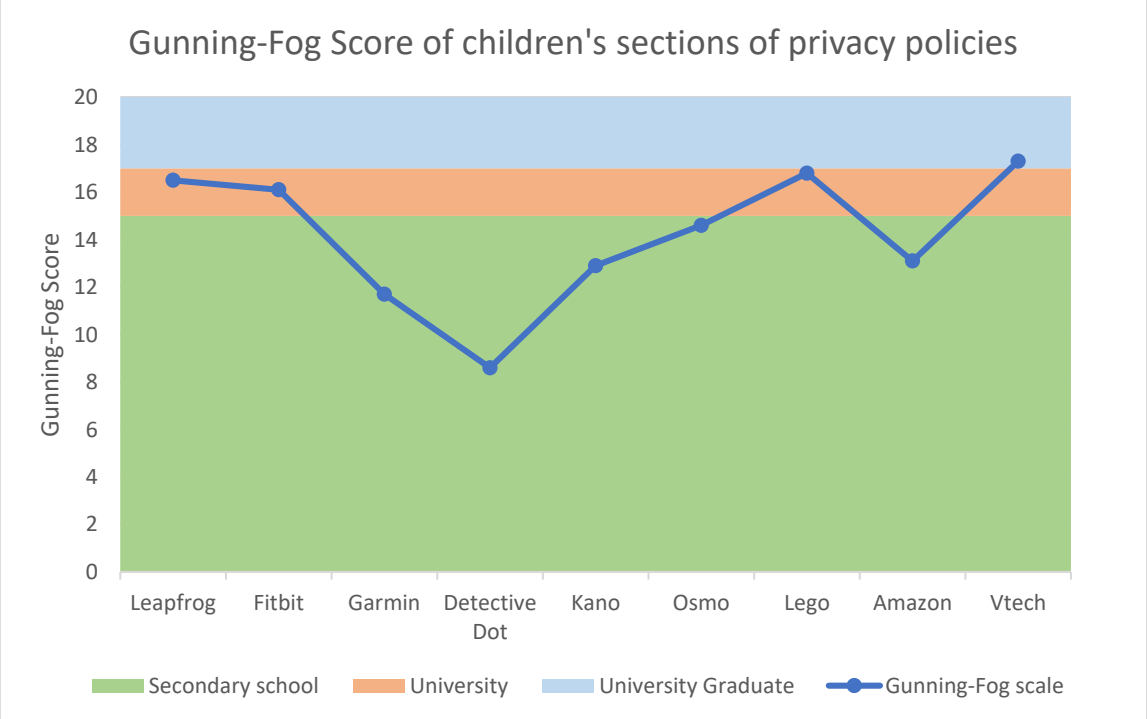
product manual (for instance, the Vtech Secret Safe Diary Visual). Of the devices, the only ones to explain the technology used were the fitness trackers. One might not expect such details as to the sensors and other technology within a device; however, details provided about the fitness trackers were particularly beneficial in showing whether or not GPS, or other location-based technologies, were included in the device.[10]

How easy is it to determine basic security and privacy measures taken by the manufacturer?

The manuals reviewed were streamlined for simplicity – often describing the core functionality in pictures and limited text and regulatory warnings (notably around battery use and potential radio interference) only. The user manuals of the connected toys did not highlight any of the points covered in the two NCSC articles or the DCMS Code of Practice, or give any suggestions as to how the user could further their knowledge in these areas.

The vast majority of connected products returned no negative new search results. Those that did (Fitbit, Amazon products) were largely because of current negative news stories at the time of research: manufacturers with known ongoing privacy concerns[11] did not return negative news articles in the first two pages of the search.

Of the 15 connected products, 13 (9 manufacturers) had privacy policies that related explicitly to children's use of the connected elements of the product. All flagged that some form of parental consent was necessary until the child was (typically) 13 years old. Using the Gunning-Fog measure of readability, the suggested educational levels to understand the sections aimed at children are:



[10] Being able to locate a child is often a matter of significant concern in terms of maintaining their personal safety.

[11] For example, VTech as the subject of a large data breach in 2016. The company continues to suggest in its most recently published privacy policy that they bear no liability for data breaches (something that is out of line with their obligations under the GDPR) (Hunt, 2016).

Although only the Detective Dot policy was specifically written for children to read, it is important to note that the majority of privacy policies may be written at a level that even the adult finds hard to comprehend.

Within the children's section of the privacy policies, three manufacturers explicitly referenced how to delete personal data; only two suggested that false details relating to children (e.g. nicknames instead of given names) should be used instead of true personal details. One connected toy (Scout My Puppy Pal) actually made a feature, in its advertising, of using the child's name as a keys means of interacting with the child.

What does the adult responsible for agreeing to the terms and conditions have to do to make the device work as intended?

Aside from the devices intended to work independently as computers or tablets, the remaining 12 connected devices required additional technology for them to work as intended, ranging from a television (the Leap TV), to smartphones to run apps, or a computer to plug the device in and perform updates. One of the devices here, Detective Dot, actually does not require any form of internet connection – but is marketed alongside an app aimed exclusively at children. The fitness trackers require a smartphone app, with two other devices needing a tablet-based app. Devices that are computers or tablets themselves have their own software, which adults need to consent to – and, in one case, the Amazon Fire Kids Tablet, must ultimately buy a paid subscription in order to maintain access to child-friendly content. Three devices have to be plugged into a computer, and registered on the manufacturer's online system.

13 of the connected products had video adverts available for review online. Themes across these adverts included the independence of the child in using the product, with eight depicting a relationship between an adult (typically a caregiver), child and the device. In the majority of these cases, the adults in the adverts highlighted the independence of the children whilst using the product (one advert showed children at childcare with the message "you can message your mum!"), with only one explicitly showing an adult setting up the device first. 12 of the adverts focused on the value of the device in improving educational attainment, and other goal setting activities (whether improved technological literacy, movement targets or chore goals) – values more likely to appeal to adults buying the product than children using it.

In all but one case, the transfer of ownership that may come at the age of consent for data processing is not addressed. One fitness tracker suggested that, at this point, the child could switch over to using their own instance of the adult app (it is not clear if the data previously gathered by the child would be associated with the new app).

One device, the Samsung Galaxy Fit (e), was included in the review despite not being designed for or marketed at children (or having appropriate privacy or parental controls). It was included in the Metro article looking at the "best fitness trackers to keep your kids active", because of its light weight and cheap price. Whether or not the device was produced for children was not a consideration in the article.

One product was still listed on amazon.co.uk despite no longer being marketed by the company (the Leapfrog Leap TV). Any purchase of these products would be without the ongoing support that one might expect of a connected device.

Discussion

Lack of Clarity

The review performed showed the **difficulty, in some circumstances, of determining whether a product marketed at children utilises smart or connected technologies directly, or needs to be supported through an app or other connected technology**. A device not clearly labelled as requiring access to a computer, smartphone or the Internet may place additional requirements upon carers that they are not expecting or willing to attend to, or that they fully understand. This is particularly important as there is no restriction on the purchase of the products, even if the use of the supporting software may have age and system limitations. Mascheroni and Holloway (2017) highlight that the ownership of connected toys is "indistinct", in that the child has ownership of the physical toy, but retains little or no rights surrounding the personal data generated. As Holloway and Green (2016) point out, agreements around data collection – even for children's data – tend to be opt-in or opt-out of the service altogether.

None of the connected toys reviewed explained how not connecting to the Internet would affect the child's ability to play with them. In the case of devices bought without clear marketing of the connectivity to the Internet – or products that are gifted to children by others – parents and carers may feel they are obliged to agree to any such terms and conditions. They may also – in the case of devices being sold second-hand - agree to owning devices that are no longer supported by the manufacturer – or whose manufacturer no longer exists.

The example of the Samsung fitness tracker also shows that **cheaper, smaller versions of adult IoT devices may be considered suitable gifts for children – even though the terms of Samsung's privacy policy for the European Union does not reference children at all**.[12] This is concerning because, once purchased, a child can use any device that their caregiver deems reasonable. Valente and Cardenas (2017) found that carers allow children full access to connected devices aimed at an adult audience, because the functionality is broader than equivalent devices aimed at children. Safeguards in place for children's privacy in particular may be of little value if toys that are marketed to them pale in comparison to technology that is already available in the child's home.

Difficulty of adult/child boundaries

Perhaps most striking from the results of the study is **the level of ongoing involvement that the adult is expected to have in the relationship that the child has with the toy.** All the connected products in the review appear to target users under 13 years old. This means that, in all cases, parental consent is needed for the personal data of the child to be collected. Furthermore, **in almost all cases, a carer will need to provide the child with access to an additional device to use the product as intended.**

Neoliberal political messaging suggests that parents have a moral obligation to devote significant effort to the upbringing of the child (Edwards and Gillies (2011)). **Connected technologies provide a mechanism to do this in a framework that adults recognise, providing the opportunity for detailed tracking of pre-determined metrics, both of educational and fitness-based attainment**. The adverts for fitness trackers in this study focused as much on the parent's ability to review achievements and set goals on the tracker as their ability to be used by children for play. Self-tracking is popular

[12] However, because of COPPA, there is a US supplement to Samsung's privacy policy that does discuss the need for parental consent.

amongst adults as understanding more about one's self can be an empowering activity when it is voluntary (Lupton, 2019).

However, in the case of the children's tracking devices reviewed here**, neither goals nor activities are necessarily voluntarily set by the child, and are shared with adults in a position of authority over them.** As Mascheroni (2017) points out, it is unclear what this might teach children about the personal ownership of data tracking their movements. Lupton (2019) goes on to say that as well as feeling empowerment, adults can often feel overwhelmed and ambivalent towards data that they have generated: it is likely that children, who may understand the data they are generating less – and have less say over generating it in the first place - will feel similar ambivalence or overwhelm. This may colour their relationship with data as they become adults. Carers are a major factor in the socialisation of consumer preferences of children (Thaichon, 2017). In giving the child access to such devices, they are also normalising the use of technology to the child. This may also go some way to explaining why the majority of connected toys in the survey either directly mimic,[13] or appear materially the same as, adult products:[14] carers understand the products, and children recognise them as valuable because they see adults using them.

Fitness trackers in particular add elements of gamification and brand lock-in into the parental consent process. The child can only use the tracker if the caregiver sets up a "family account" – under the expectation that at least one of the child's carers has an adult equivalent device (from the same manufacturer). The family account feature not only enables the child to use the device, but provides the parent with access to the child's collected data (and, for some devices, allows for the caregiver to set chores and other reminders for the child). The use of family accounts as a means of confirming parental consent for the collection of a child's personal data has been shown to be inflexible and often, insensitive towards non-nuclear familial structures, familial breakdown and restructure (Goulden, 2019). In addition, it has been shown – in social media settings – that children and teenagers are aware of the need to curate specific profiles depending upon their audience, as the concept of privacy can be fluid – and easily invaded (Boyd, 2015). **It is unclear how using devices that expect the sharing of personal information with authority figures might sit with slightly older children who are becoming aware of their personal privacy boundaries.** Children do expect to be able to retain control over their data, and retain agency in relation to its use (Coleman et al., 2017): this may particularly cause tensions in situations of familial breakdown, or restructure, when adults may suddenly no longer be privy to – or conversely, suddenly become privy to – this personal data.

The occasion of a child turning 13 may present further complexities as well – as an adult, the teenager would be entitled to be removed from the family account and take ownership of their own account. This presupposes, however, that the teenager has access to their own, separate smart phone or tablet to use for the app. Realistically, this is likely to be the case (with 83% of 12-15 year olds in the UK having their own smartphone)[15], but is an assumption as to the willingness and ability of the family to provide access to such a device. **This allowance also suggests a step-change in the ability of the 13-year old to understand the terms of the use of the device.** The reading age of the privacy policies read in this review – even if only for the children's sections – suggests that this expectation may not match up with reality.

[13] 6 in total, plus the Samsung device, which is actually intended for adults
[14] 2 tablets (Amazon Fire and VTech), plus the Kano computer
[15] Ofcom (2019)

Independence…at the cost of privacy and security?

Of the connected products reviewed in the survey, the majority of those that were not directly mimicking adult technology were focused on the acquisition of knowledge around technology.[16] These products more directly complement the UK's Key Stage One and Two curricula, by allowing children to code simple algorithms.[17] The focus on education, as showed in the adverts that were reviewed, also **highlights the potential that connected toys give for a positive, independent experience for the child**.[18] This message is one that carers may be particularly keen to hear, as caregiver's devices are often offered as a means to keep the attention of a child whilst the adult is busy with something else (Livingstone, 2015).

Children are less likely than a parent or carer to understand the implications of bringing a connected device into the home. **Research has shown that children do not always understand that devices with a microphone will record them**, or that individuals can subsequently listen to the recordings (Valente and Cardenas (2017)). Although Article 14 of GDPR suggests that privacy policies should be targeted at the users of the product, this does not happen in practice – with only one of the six privacy policies reviewed having a reading age close to the target age of the product (Detective Dot being aimed at children aged 7+). **Combining a lack of understanding with an insecure product has the potential to facilitate malicious activities (Chu et al., 2019) or unintended consequences** – for example, the smart device that could be used inadvertently to order products from Amazon (Laughlin, 2017).

Realistically, carers will not read the privacy policies either (Obar & Oeldorf-Hirsch (2018)), and, as mentioned above, may struggle to understand them in any case. **Privacy policies are meant to be an individual's primary means of understanding how – amongst other things – to delete data that is stored with a data controller. This is particularly important in terms of devices that are bought for children, that may get donated, re-gifted or otherwise handed over to others** when the child outgrows it. 13 of the 15 connected toys in this research did not provide clear information in the privacy policy about how to delete personal data. In both cases, **deleting data requires sending an email or other message to the manufacturer; it is not an automatic process** (for example, being able to delete through pressing a button on the app or website associated with the device). This is not ideal, as email is a slow and complex way for an individual to communicate with an organisation – having to draft an email with appropriate words is much more time-consuming and labour-intensive than pressing a button designed for this purpose. Valente and Cardenas (2017) show the relative ease with which data can be gained from a connected, smart toy – you can ask it questions that may point to a name, location, or other distinguishing features of the previous owner.

Conclusions and recommendations

This research confirms earlier work that show the several issues that connected toys create between children and carers. The framework that is imposed in order to protect the children's privacy – in the shape of the additional requirements of the GDPR, and COPPA – paradoxically seem to have created a series of products where, in order to meet the requirements of the law, the privacy of the child is often reduced. This may be an appropriate trade off, in order to secure children from the darkest issues that stolen personal information can create. However, there is little guarantee that impeding this privacy will lead to better outcomes. Children's personal data has been poorly stored

[16] For example, devices furthering knowledge of coding, such as Osmo
[17] Department for Education (2013)
[18] In the advert, Scout the puppy is used to entertain the toddler independently, as well as be a bedtime companion (instead of the parent).

in the past; the lack of adherence to codes of conduct to explain the security measures adhered to means it is hard to be sure of the security of devices brought into the home for children to play with.

In assessing any device – but particularly one designed to be given to children, it is suggested that carers consider the following points prior to purchase.

- Do I know how it connects to the internet? If the device connects to a home Wi-Fi network, am I happy with all the individuals who have the password to that network?
- Do I understand what personal data the device, and any associated software, uses in relation to my child? Where would it make sense to use fake data (such as nicknames)?
- Does my child understand what I can see of their data? Are they happy with how I use that data?
- Can I delete the child's data once the toy is no longer actively used?
- Can the child's data be moved to an adult account, should they be using the device once they hit the age of data processing consent? Do I know what the difference between the child and adult app is?

Furthermore, it would be of significant value if manufacturers made more publicly available information relating to the security and privacy of those products that are targeted at children. Publicly stated compliance with a recognised code of practice or conduct might be a simple way to show the measures in place. In lieu of this, it would be beneficial for manufacturers to:

- Clearly state on the packaging and in the manual where a toy requires connection to the Internet, and explain within the manual what functionality is lost should a toy not be connected.
- Point users to recognised cyber-hygiene and security guidance within the documentation.[19]
- Do not require children's names or ages as part of the registration/account naming process; rather recommend the use of pseudonyms.
- Clearly state in the manual what data is collected about the child, how this is held, and for what purpose.
- Make the default option for selling or give a child's data to third parties, particularly for advertising purposes, opted out. Opting out of such data processing should not encroach on the functionality of the toy.
- Clearly explain the methods of removing all personal data from the device/relevant data storage mechanisms, coupled with a clearly available take out and deletion mechanism.[20] This should be instantaneous, and should not involve email or other personal contact with individuals or teams at the manufacturer.

[19] Such as National Cyber Security Centre's guidance pages "Smart Devices: using them safely in your home" (2109) and "Top tips for stay secure online" (2018)

[20] See, for example, the user functionality in Google's Download Your Data tool (https://takeout.google.com/)

References

"Code Of Practice For Consumer IoT Security". GOV.UK, 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747413/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf. Accessed 26 Nov 2018.

"Top Tips For Staying Secure Online". National Cyber Security Centre, 2018, https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online. Accessed 22 Nov 2019.

"Leading Search Engines Ranked By Market Share UK 2019 | Statista". Statista, 2019, https://www.statista.com/statistics/280269/market-share-held-by-search-engines-in-the-united-kingdom/. Accessed 28 Aug 2019.

"Smart Devices: Using Them Safely In Your Home". National Cyber Security Centre, 2019, https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home. Accessed 22 Nov 2019.

Blythe, John M et al. "What Security Features And Crime Prevention Advice Is Communicated In Consumer IoT Device Manuals And Support Pages?". Journal Of Cybersecurity, vol 5, no. 1, 2019. Oxford University Press (OUP), doi:10.1093/cybsec/tyz005. Accessed 22 Nov 2019.

Blythe, John, and Shane Johnson. Rapid Evidence Assessment On Labelling Schemes And Implications For Consumer IoT Security. PETRAS IoT Hub, 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/775562/Rapid_evidence_assessment_IoT_security_oct_2018.pdf. Accessed 30 Apr 2019.

Boyd, Danah. It's Complicated. Yale University Press, 2015.

Chu, Gordon et al. "Security And Privacy Analyses Of Internet Of Things Children's Toys". IEEE Internet Of Things Journal, vol 6, no. 1, 2019, pp. 978-985. Institute Of Electrical And Electronics Engineers (IEEE), doi:10.1109/jiot.2018.2866423. Accessed 24 Nov 2019.

Coldeway, Devin. "After Breach Exposing Millions Of Parents And Kids, Toymaker Vtech Handed A $650K Fine By FTC – Techcrunch". Techcrunch, 2018, https://techcrunch.com/2018/01/08/after-breach-exposing-millions-of-parents-and-kids-toymaker-vtech-handed-a-650k-fine-by-ftc/. Accessed 22 Nov 2019.

Coleman, Stephen et al. The Internet On Our Own Terms: How Children And Young People Deliberated About Their Digital Rights. 5Rights, 2017, https://5rightsfoundation.com/static/Internet-On-Our-Own-Terms.pdf. Accessed 26 Nov 2019.

Department for Education. The National Curriculum In England: Key Stages 1 And 2 Framework Document. 2013, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/425601/PRIMARY_national_curriculum.pdf. Accessed 25 Nov 2019.

Edwards, Rosalind, and Val Gillies. "Clients Or Consumers, Commonplace Or Pioneers? Navigating The Contemporary Class Politics Of Family, Parenting Skills And Education". Ethics And Education, vol 6, no. 2, 2011, pp. 141-154. Informa UK Limited, doi:10.1080/17449642.2011.622982. Accessed 22 Nov 2019.

Forbrukerradet. #Toyfail: An Analysis Of Consumer And Privacy Issues In Three Internet-Connected Toys. 2016, https://fil.forbrukerradet.no/wp-content/uploads/2016/12/toyfail-report-desember2016.pdf. Accessed 22 Nov 2019.

Future of Privacy Forum and Family Online Safety Institute. Kids And The Connected Home: Privacy In The Age Of Connected Dolls, Talking Dinosaurs, And Battling Robots. 2016, https://fpf.org/wp-content/uploads/2016/11/Kids-The-Connected-Home-Privacy-in-the-Age-of-Connected-Dolls-Talking-Dinosaurs-and-Battling-Robots.pdf. Accessed 22 Nov 2019.

Goulden, Murray. "'Delete The Family': Platform Families And The Colonisation Of The Smart Home". Information, Communication & Society, 2019, pp. 1-18. Informa UK Limited, doi:10.1080/1369118x.2019.1668454. Accessed 22 Nov 2019.

Hunt, Troy. "No, Vtech Cannot Simply Absolve Itself Of Security Responsibility". Troy Hunt, 2016, https://www.troyhunt.com/no-vtech-cannot-simply-absolve-itself/. Accessed 22 Nov 2019.

Knowles, B. et al. "What Children's Imagined Uses Of The BBC Micro:Bit Tells Us About Designing For Their IoT Privacy, Security And Safety". Living In The Internet Of Things: Cybersecurity Of The IoT - 2018, 2018. Institution Of Engineering And Technology, doi:10.1049/cp.2018.0015. Accessed 22 Nov 2019.

Laughlin, Andrew. "Smart Toys - Should You Buy Them? - Which?". Which?, 2017, https://www.which.co.uk/reviews/toys/article/smart-toys-should-you-buy-them. Accessed 25 Nov 2019.

Lupton, Deborah. "Data Mattering And Self-Tracking: What Can Personal Data Do?". Continuum, 2019, pp. 1-13. Informa UK Limited, doi:10.1080/10304312.2019.1691149. Accessed 24 Nov 2019.

Mascheroni, Giovanna, and Donell Holloway. The Internet Of Toys: A Report On Media And Social Discourses Around Young Children And Iotoys. Digilitey, 2017, http://digilitey.eu/wp-content/uploads/2017/01/IoToys-June-2017-reduced.pdf. Accessed 22 Nov 2019.

Morris, Natalie. "The Best Fitness Trackers For Kids | Metro News". Metro.Co.Uk, 2019, https://metro.co.uk/2019/08/15/the-best-fitness-trackers-to-help-keep-your-kids-active-10569887/. Accessed 22 Nov 2019.

Ni Loideain, Nóra. "A Port In The Data-Sharing Storm: The GDPR And The Internet Of Things". Journal Of Cyber Policy, vol 4, no. 2, 2019, pp. 178-196. Informa UK Limited, doi:10.1080/23738871.2019.1635176. Accessed 22 Nov 2019.

Obar, Jonathan A., and Anne Oeldorf-Hirsch. "The Biggest Lie On The Internet: Ignoring The Privacy Policies And Terms Of Service Policies Of Social Networking Services". Information, Communication & Society, 2018, pp. 1-20. Informa UK Limited, doi:10.1080/1369118x.2018.1486870. Accessed 24 Nov 2019.

Ofcom. Children And Parents: Media Use And Attitudes Report 2018. Ofcom, 2019, https://www.ofcom.org.uk/__data/assets/pdf_file/0024/134907/children-and-parents-media-use-and-attitudes-2018.pdf. Accessed 24 Nov 2019.

Thaichon, Park. "Consumer Socialization Process: The Role Of Age In Children's Online Shopping Behavior". Journal Of Retailing And Consumer Services, vol 34, 2017, pp. 38-47. Elsevier BV, doi:10.1016/j.jretconser.2016.09.007. Accessed 24 Nov 2019.

Valente, Junia, and Alvaro A. Cardenas. "Security & Privacy In Smart Toys". Proceedings Of The 2017 Workshop On Internet Of Things Security And Privacy - IoTs&P '17, 2017. ACM Press, doi:10.1145/3139937.3139947. Accessed 24 Nov 2019.

Yeoman, Fran. "10 Best Coding Toys". The Independent, 2017, https://www.independent.co.uk/extras/indybest/kids/gifts/best-coding-toys-for-kids-games-2017-apps-software-laptop-robot-for-beginners-a8029061.html. Accessed 22 Nov 2019.