ABSTRACT

Villain or Guardian? “The smart toy is watching you now….”

:Smart toys, because they collect and have the facility to share data, have been viewed as surveillance devices, being banned in some countriesand cast as villains. But who are they spying for? Could we imagine a smart toy that is programmed to pick up concerns raised by the child about their treatment by parents or guardian and alert the authorities? Could they be used to positive effect, therefore? It will be argued that this isa complex and contested area and there are clear contradictions in law, particularly concerning the protection of a child’s right to privacy versus parental expectations.Thisarticle therefore challenges some of the narrativesaround thisarea.The article will also ask whether the smart toy offersan opportunity to recast the notion of a child’s right to privacy in a way that balances children’sautonomy rights with their protection rights. It is often the unintended use of technology that shifts its purpose from villain to guardian and backagain,and the smart toy may be anotherexample of this.

KEY WORDS

Smart / connected toys, privacy (children), data protection, state intervention

Dr Lisa Collingwood
Kingston University
Law Department
Lisa.collingwood@kingston.ac.uk
0208 417 5210

Introduction

Toys of a new kind are appearing on the shelves of toys shops. These technologically-enhanced toys, or smart toys, have become a global phenomenon, changing the way that children play. These toys incorporate internet technologies that respond and relate to children[1]. Included in this category are, inter alia, watches, robots, talking dolls or teddy bears. All share the facility to be connected to the internet and therefore remote servers that collect data and power the toy's intelligence[2]. Some of these toys are also able to adapt to the actions of the user, to be 'smart', in other words[3]. For example, My Friend Cayla, an interactive doll that users can talk to, uses speech recognition, a microphone and speakers to understand what a user is saying. The internet-connected toy submits the user's queries through a Bluetooth connection to a smartphone app to come up with responses[4] and she can whisper to children in several languages (using Google Translate) that she's great at keeping secrets, for example. The resultant play data can be captured by the device and stored either in the Cloud or locally (in the device itself). Effectively, the toy manufacturers own the harvested data, as specified in the product's terms of use and they appear to have the facility to share it[5]. Herein lies the problem. The functionality of these toys enables a data exchange between multiple stakeholders which is accompanied by a largely undefined set of risks and concerns. The recognized vulnerability of children combined with the increasing volume of use requires action to ensure protection for children and their data[6]. This is because the rise of these toys has made children vulnerable in ways their parents may not have imagined[7]. Not only are there a range of risks associated with this technology because of the inherent data capture, but there are also unexpected consequences due

[1] Giovanna Masheroni and Donell Holloway (Eds) 2017 The Internet of Toys: A report on media and social discourses around young children and IoToys < http://digilitey.eu/wp-content/uploads/2017/01/IoToys-June-2017-reduced.pdf > accessed 14 February 2020
[2] Future of Privacy Forum - Family Online Institute (FOSI), *Kids & the connected home: privacy in the age of connected dolls, talking dinosaurs and battling robots,* 2016, page 2
[3] Stephane Chaudron et al, 'Kaleidoscope on the Internet of Toys' [2017] JRC Technical Reports, page 11 <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC105061/jrc105061_final_online.pdf> last accessed 14 February 2020
[4] https://www.snopes.com/news/2017/02/24/my-friend-cayla-doll-privacy-concerns/
[5] Stephane Chaudron et al, 'Kaleidoscope on the Internet of Toys' [2017] JRC Technical Reports, page 11 <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC105061/jrc105061_final_online.pdf> last accessed 14 February 2020.
[6] ibid
[7] https://www.bayshorenetworks.com/blog/2015/12/vtech-hack-shows-why-parents-have-to-stay-ahead-of-the-game/, last accessed 19 September 2018. See below.

to the ways in which the data is effectively masked. This article, therefore, explores these unexpected outcomes before focusing on the risks to children's (informational) privacy. In so doing, it challenges several of the narratives in this area and then proceeds to examine the role of the various responsible bodies in protecting information collected from and about children, querying whether the law as currently developed is fit for purpose in this context. The rationale for this is that, whilst there is legislation in place in the jurisdictions covered in this article that protects data generally, since smart toy technology arguably infringes one of the most intimate aspects of a child's life, it is questionable whether data protection law as currently developed is able to respond adequately to the risks to informational privacy posed by smart toy technology. Further, since it is a child's right to privacy (as opposed to data protection) that is ultimately at stake, this article also critiques the reach of misuse of information law, evaluating the effectiveness of both data protection legislation and misuse of private information in protecting children's rights.

It is clear that smart toys represent an emerging and lucrative market for toy vendors[8]. Internet connected toys can be bought and sold to children across the world. It is estimated that the size of the global toy market is more than 87 billion U.S. dollars annually, of which about one quarter can be attributed to the North American market[9]. Given the magnitude, it is perhaps unsurprising thatthere has been a global response to the risks posed to children by the new generation of smart toys. Therefore, an evaluation of key responses and initiatives is also provided herein.

Risks to childhood

Prior to evaluating the various issues connected with smart toys, it is necessary to define certain terms:-

A "smart toy" has been defined as a device consisting of a physical toy component that connects to one or more computing services to facilitate gameplay in the Cloud through

[8] Sam Smith, 'Smart Toy Revenues to Hit $28BN This Year' (Juniper Research, 2015) <https://www.juniperresearch.com/press/press-releases/smart-toy-revenues-to-hit-$2-8bn-this-year>
[9] https://www.statista.com/statistics/194424/amount-spent-on-toys-per-child-by-country-since-2009/, last accessed 19 September 2018

networking and sensory technologies to enhance the functionality of a traditional toy[10]. These toys typically contain sensors, microphones, cameras, data storage components, and other multimedia capabilities—including speech recognition and GPS options in some cases[11]. As stated above, children share their secrets with their smart toys and, inherent within such devices is the ability to collect the information gathered from the child during play (the child's "play data"). It is this functionality that causes risks to both children's safety and their informational privacy because of concerns about how the play data is used for "data analysis purposes" (see below). "Informational privacy" is broadly defined and conceptualising a privacy value is not straightforward. However, since the first explicit legal analysis of privacy was formulated by Warren and Brandeis[12], it is prudent to start here, although it should be mentioned that the early exposition provided by Warren and Brandeis has been widely critiqued by the likes of Posner[13], Prosser[14], Westin[15], Gavison[16], Rachels[17] and Zimmermann[18] to name just a few of the key privacy theorists and scholars. Warren and Brandeis regarded privacy as the "right to be left alone". Central to this notion is the ability of individuals to keep society and the State at arms length, and to obtain a remedy where there has been an unwanted intrusion[19]. According to Warren and Brandeis, such a remedy would be forthcoming from the common law for it was this that protected an individual's entitlement to decide the extent to which thoughts, sentiments and emotions should be communicated to others[20]. Put into a more contextual framework, this idea may correspond to many of the conventional understandings of privacy, such as 'a man's home is his castle'[21], reflecting the societal desire to avoid the prying eyes of others. With these definitions in mind, it will be possible to consider both the risks inherent

[10] Jeff K.T. Tang (Editor), Patrick C. K. Hung (Editor), Computing in Smart Toys (Springer International Publishing) 2017, 1.
[11] https://www.wired.com/story/dont-gift-internet-connected-toys/, last accessed 28 September 2018
[12] Warren, S and Brandeis, L 'The right to privacy' (1890) 4 *Harvard Law Review* 193.
[13] Posner, R, 'An economic theory of privacy', [1978] *Regulation* (May/June) 19
[14] Prosser, W, 'Privacy' (1960) 48 *California Law Review* 383.
[15] Westin, A, *Privacy and Freedom* (Atheneum 1967).
[16] Gavison R, 'Privacy and the limits of the law', (1980) 89 *Yale Law Journal* 421.
[17] Rachels, J, 'Why Privacy is important' 1975 4(4) *Philosophy and Public Affairs* 323.
[18] Zimmerman, D 'Requiem for a Heavyweight : A Farewell to Warren and Brandeis's Privacy Tort" (1983) 68 *Cornell Law Review* 291.
[19] Raab, C and Goold, B, *Protecting Information Privacy* (Equality and Human Rights Commission Research Report 69, 2011) 16.
[20] Warren, S and Brandeis, L 'The right to privacy' (1890) 4 *Harvard Law Review* 193, 198
[21] Raab, C and Goold, B, *Protecting Information Privacy* (Equality and Human Rights Commission Research Report 69, 2011) 16.

with smart toys and the ways in which data protection and misuse of private information law may be able to overcome the informational privacy challenges posed by them.

At the outset, it may be stated that a range of threats, which could put the privacy and safety of children at risk, attach to smart toys. Of major concern is that children form friendships with these toys and confide intimate details about their lives to them. This raises risks, including: -

- Data security (biographical data – voice is unique to a person)
- Device security (toy can be hijacked to behave badly or erratically)
- Device security (geolocational tracking of children)
- Children's privacy (secrets recorded/monitored, incremental effect of data collection and sharing over a lifetime)[22].

Such risks arguably mean that children may become increasingly vulnerable to harassment, stalking, grooming, sexual abuse or exploitation[23], as well as personal data misuse[24], as detailed below.

Protection of children's personal information

Clearly the protection of a child's personal information is not a new phenomenon. Children's rights are in fact firmly entrenched in various ways. For example, as detailed below, in the EU, via means of the General Data Protection Regulation (GDPR[25]) and in the US via the Children's Online Privacy Protection Act (COPPA). Most often, parents or guardians have legal responsibility for the dissemination of their children's personal information and must provide consent to the use of services in cases where the child is a minor. In the case of smart toys, the information disclosure practices are outlined in their privacy policy, with parents/guardians being required to provide their consent on behalf of their children. Armed with parental consent, smart toy manufacturers can essentially use the information gathered from the child during play

[22] FN 1, page 9
[23] Jeff K.T. Tang (Editor), Patrick C. K. Hung (Editor), Computing in Smart Toys (Springer International Publishing) 2017, 2.
[24] See also Ivan Gudymenko and others, 'Privacy Implications of the Internet of Things' [2012] 277(1) Communications in Computer and Information Science <https://doi.org/10.1007/978-3-642-31479-7_48> accessed 27 March 2018 p281-282
[25] Milda Macenaite and Eleni Kosta, 'Consent for processing children's personal data in the EU: following in US footsteps?'[2017] 26(2) Information & Communications Technology Law <https://doi.org/10.1080/13600834.2017.1321096>

(the play data) for any purpose that it chooses, invariably under the heading "data analysis purposes" or similar. The information is effectively both actively and passively gathered – i.e. the toy can both passively track interactions but also actively seek information from the child – for example, by asking the child, "what is your name?" There is now growing evidence that many individuals who provided consent on behalf of their children were unaware of the pervasive nature of the policies they signed up to, having not read or understood them[26]. This produces the effect that, in an effort to protect children, responsibility is shouldered with parents and this arguably has the potential to limit *instead of* empower children.

Toymakers are regulated in the US by the Children's Online Privacy Protection Act (COPPA), which is seen as the standard worldwide. The US Federal Trade Commission (FTC) updated its COPPA compliance guidance to explicitly clarify that smart toys were included, in June 2017 (specifically those relating to voice-enabled services and applications – i.e. it added audio files that contain a child's voice to the definition of personal information). COPPA also has specific "long arm" jurisdiction and gives the FTC authority over non-U.S. entities that collect personal information from U.S. children[27]. COPPA applies to operators of websites and online services (which may include connected home devices, wearables, toys, and mobile apps) that obtain personal information from children under the age of thirteen; it imposes restrictions on the collection, use, and sharing of such personal information, requiring notice and parental consent absent certain limited exceptions. The COPPA Rule covers sites and services that are directed to children as well as those that are not targeted to children, but have actual knowledge that they are collecting personal information from children[28]. However, while COPPA puts limits on data-harvesting, it mostly ensures that parents have to give consent before data collection happens. In the frenzy of setting up a Christmas gift, it's easy to tap 'yes' without realizing exactly what it is you've agreed to[29] and there are now several allegations that smart toys record children's

[26] Jeff K.T. Tang (Editor), Patrick C. K. Hung (Editor), Computing in Smart Toys (Springer International Publishing) 2017, 2.
[27] https://www.dataprivacymonitor.com/coppa/toying-with-childrens-data-lessons-from-the-ftcs-first-connected-toys-settlement-action/
[28] https://www.dataprivacymonitor.com/coppa/from-the-mouths-of-babes-ftc-issues-coppa-enforcement-policy-regarding-voice-recordings/
[29] https://www.wired.com/story/dont-gift-internet-connected-toys/

conversations without parental consent, in violation of COPPA[30]. Under COPPA, the potential repercussions in the U.S. for failing to adequately secure children's personal information can be significant. For example, on Jan. 8, 2018, the US Federal Trade Commission (FTC) settled its first-ever connected toy privacy case with Hong Kong-based VTech Electronics, Ltd., (VTech), resulting in a $650,000 penalty. VTech was found to have collected digital data on 638,000 children — including text messages, photos, and audio messages — without notifying users or asking parents for permission to collect that information and failed to keep that information secure from hackers[31].

Whilst COPPA is arguably an effective piece of legislation that protects the privacy rights of minors under the age of thirteen (note that children can lie about their age and it is realistic to assume that circumventing age verification mechanisms is a very real possibility and COPPA, GDPR are powerless to prevent that), it has its limitations - it focuses on what data can be collected from children and restricting how it can be used by marketers, rather than securing it from hackers, for example, nor does it mandate the use of any particular technologies to defend against cyber attack. Instead, it advises that companies must have "reasonable" procedures and it appears that there is no consensus on what is reasonable[32]. It is somewhat unsurprising, therefore, that it has recently been announced that the US Federal Trade Commission is to review the operation of COPPA[33].

This is to be welcomed, but it remains there are now several instances in which smart toys have been regarded as open to hackers, spies and identity thieves[34] and, once hackers are in, they can use the toys' cameras and microphones to potentially see and hear whatever the toy sees and hears. In fact, consumer advocacy group Which? found flaws in Bluetooth and wifi-enabled toys that could enable a stranger to talk to a child

[30] Jeff K.T. Tang (Editor), Patrick C. K. Hung (Editor), Computing in Smart Toys (Springer International Publishing) 2017, 3.
[31] See https://mobile.nytimes.com/2018/01/08/business/vtech-child-privacy.html
[32] VTech hack shows why parents have to stay ahead of the game
Kuchler, H, Financial Times, London (UK) 02 Dec 2015
[33] https://www.ftc.gov/news-events/blogs/business-blog/2019/07/new-block-kids-ftc-announces-coppa-review-workshop, last accessed 14 February 2020.
[34] https://www.nytimes.com/2017/12/21/technology/connected-toys-hacking.html?rref=collection/sectioncollection/technology&action=click&contentCollection=technology&region=rank&module=package&version=highlights&contentPlacement=2&pgtype=sectionfront

in four out of the seven devices tested. [35]. In addition, very little technical know-how was needed to gain access to the toys to start sharing messages with a child. It called for retailers to stop selling toys with proven security issues[36]. The UK's Information Commissioner's Office has also warned that smart toys that will typically be sold during the Christmas shopping season could put the privacy and safety of children at risk[37]

Such comments reinforce the parental role in providing consent to use their children's information, which is clearly recognised in European Union legislation - Article 8 GDPR[38], which came into force on May 25, 2018[39], authorises parents to provide consent to the use of information society services in cases where the child is deemed too young to do so themselves[40].

The effect of Article 8 is that, where a child is below the age of sixteen years, processing of their personal data is only lawful when consent is provided by the authorised holder of parental responsibility over the child. The methodology behind this approach being that protection for children requires them to be designated as separate from adults as a result of recognising their cognitive differences and subsequent need for additional requirements[41]. Arguably, this represents an improvement from the previous Data Protection Directive 95/46/EC (DPD), which made no specific mention of children and represented all ages as a single version of a data subject. However, this is not the same as saying that the GDPR actually empowers children at all while protecting their data as it takes consent away from children and gives it to others, representing an unexpected outcome of the designation policy. Article 8 is based on the perception that a parent would naturally be better positioned then any child to make correct determinations about best use of a child's data. However, what if a parent/guardian are actually the perpetrators of harm in some way? If they are, then toys which are able to operate as

[35] https://www.theguardian.com/technology/2017/nov/14/retailers-urged-to-withdraw-toys-that-allow-hackers-to-talk-to-children
[36] https://www.theguardian.com/technology/2017/nov/14/retailers-urged-to-withdraw-toys-that-allow-hackers-to-talk-to-children, last accessed 18 September 2018
[37] https://www.teiss.co.uk/news/vtech-connected-toys-security/, last accessed 19 September 2018
[38] Covering conditions applicable to children's consent in relation to information society services
[39] GDPR Portal: Site Overview' (EUGDPR.org, 2018)<https://www.eugdpr.org, last accessed 14 February 2020
[40] See http://www.privacy-regulation.eu/en/article-8-conditions-applicable-to-child's-consent-in-relation-to-information-society-services-GDPR.htm, last accessed 17 September 2018.
[41] Information commissioner's office, 'Children as Internet users: how can evidence better inform policy debate?' (ICO, 2018) <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/applications/children/, last accessed 14 February 2020.

spying devices are capable of picking up that harm and alerting authorities. These toys would not present harm to the child, then, but to others – be they parents, carers etc. This is particularly relevant to children's toys, which are traditionally used in the most private of locations, many times in the safe space of their bedroom. So, is the banning of toys like My friend Cayla really in the best interests of the child? Perhaps children's interests and needs cannot be readily assumed to be aligned with those of their parents, carers after all[42].

While the specific mention of a child as defined by age is found in data protection legislation, it appears that the approach taken by legislators may not have taken into consideration that harm can be inflicted by those entrusted with protection and, further, that children function within varying levels of ability and knowledge in regards to the online sphere[43]. The point to emphasise here is that assumption that a parent is more qualified than a child to make decisions about collection and use of data is not rooted in any empirical research[44]. Nor is the belief that parents always represent the best interest of their child. Sometimes they may not. Adults can, and, sadly, do, harm children. Should adults therefore be entrusted with protecting children in this way at all? Or, to put it another way, does a smart toy, having the ability to constantly record and capture moments in childhood development, actually represent a positive response?

Discussions on smart toys certainly suggest that the collection of data from children eats away at their privacy and is, by definition, problematic. Yet, could we view smart toys as akin to police body cameras? These can both infringe privacy, but may also exonerate suspects and even hold police accountable. Therefore, the switching off of such cameras would become the problem rather than their presence. By extension, it is arguable that privacy and data protection regulation in relation to children in general, and smart toys in particular, has actually also caused them harm (child abuse, institutional sex abuse etc) because the associated lack of data or records has operated

[42] Joseph Savirimuthu, 'EU General Data Protection Regulation Article 8: Has Anyone Consulted the Kids' (Media Policy Project Blog, 1 March)<http://blogs.lse.ac.uk/mediapolicyproject/2016/03/01/eu-general-data-protection-regulation-article-8-has-anyone-consulted-the-kids, last accessed 14 February 2020.

[43] Gerison Lansdown, The Evolving Capacities of Children. [2005] Florence: UNICEF Innocenti Research Centre.

[44] Simone van der hof and Eva Lievens, 'The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR' [2018] 23(1) Communications Lawhttps://ssrn.com/abstract=3107660, last accessed 14 February 2020.

to protect adult perpetrators. Scholars have acknowledged that paternalistic protection is a favoured approach under data protection regulation[45], but placing children under the strict overprotection of their parents or guardians may not be in their best interests and questions about the short-sightedness of legislators have been raised and conclusions drawn that data protection policy is out of touch with the needs of children in the digital age[46].

Therefore, the very narrative of the data protection legislation can be challenged[47] because the *intention* of the data protection legislation and the *reality* of its implementation in achieving the goal of protecting children may not always be the same. In other words, as detailed above, there are unexpected outcomes. This explains why Article 8 has been met with indignation and disbelief by children's rights campaigners and advocates[48].

The EU's commissioner for justice, consumers and gender equality, Vera Jourová has said that she had concerns about the impact of smart dolls on children's privacy and safety and Germany's telecommunications watchdog ordered parents to destroy or disable a "smart doll" because it could be used to illegally spy on children….[49] The toy in question was the My Friend Cayla interactive doll. In 2017, after researcher Stefan Hessel had alerted Germany's Bundesnetzagentur (Federal Network Agency, the country's regulatory office) about the security issues and potential capabilities of the smart toy, Cayla was labelled as "an illegal espionage apparatus"[50]. It was stated that hackers could use the doll to steal personal data by recording private conversations over

[45] H Stalford, Children and the European Union: Rights, Welfare and Accountability [2012] Oxford: Hart Publishing
[46] Joseph Savirimuthu, 'EU General Data Protection Regulation Article 8: Has Anyone Consulted the Kids' (Media Policy Project Blog, 1 March)<http://blogs.lse.ac.uk/mediapolicyproject/2016/03/01/eu-general-data-protection-regulation-article-8-has-anyone-consulted-the-kids/last accessed 14 February 2020.
[47] 'The General Data Protection Regulation and children's rights: questions and answers for legislators, DPAs, industry, education, stakeholders and civil society' [2017] Better Internet for Kids<https://www.betterinternetforkids.eu/documents/167024/2013511/GDPRRoundtable_June2017_FullReport.pdf/e6998eb6-ba3c-4b5d-a2a6-145e2af594f2, last accessed 14 February 2020.
[48] Joseph Savirimuthu, 'EU General Data Protection Regulation Article 8: Has Anyone Consulted the Kids' (Media Policy Project Blog, 1 March)<http://blogs.lse.ac.uk/mediapolicyproject/2016/03/01/eu-general-data-protection-regulation-article-8-has-anyone-consulted-the-kids/, last accessed 14 February 2020.
[49] https://www.theguardian.com/world/2017/feb/17/german-parents-told-to-destroy-my-friend-cayla-doll-spy-on-children
[50] Press Release, 'Bundesnetzagentur removes children's doll "Cayla" from the market' (Bundesnetzagentur, 17 February 2017)

an insecure Bluetooth connection[51]. Under the German Telecommunications Act it is illegal to sell or possess a banned surveillance device and as the authorities determined that Cayla amounted to a concealed transmitting device she was therefore banned. It was recommended that parents destroy the doll and German retailers were told they could sell the doll only if they disconnected its ability to connect to the internet, the feature that also allows in hackers. For similar reasons, it subsequently banned the sale of smartwatches aimed at children, describing them as spying devices[52]. Since then, several security researchers have raised concerns over what type of data the doll collects, and how the data is used[53]. Cybersecurity experts reiterate the view that, since smart toys all connect with the internet to interact, it is straightforward to use them in order to spy on children[54] and also to use the toy in order to access the personal data, such as bank details etc, of parents / guardians[55].

In the international arena, we have recently seen the drafting of a General Comment on children's rights in relation to the digital environment by the Committee on the Rights of the Child.[56] Findings from the Global Treat Assessment (WePROTECT Global Alliance) confirm that online child sexual exploitation and abuse – in its scale, severity and complexity – is increasing faster than its prevention and response[57]. The UK's Information Commissioner's Office is in the process of putting together an age-appropriate design code, which will outline the standards that providers of online services which process personal data and are likely to be accessed by children will be expected to meet[58].

---

[51] https://mobile.nytimes.com/2017/02/17/technology/cayla-talking-doll-hackers.html?emc=edit_th_20170219&nl=todaysheadlines&nlid=55059608&referer=
[52] http://www.bbc.co.uk/news/technology-42030109
[53] See also http://www.dailymail.co.uk/sciencetech/article-5714587/From-secret-spying-kids-chatting-terrifying-ways-smart-toys-hacked.html, last accessed 15 August 2018.
[54] https://www.nytimes.com/2017/12/21/technology/connected-toys-hacking.html?rref=collection/sectioncollection/technology&action=click&contentCollection=technology&region=rank&module=package&version=highlights&contentPlacement=2&pgtype=sectionfront
[55] https://teiss.co.uk/information-security/internet-connected-toys-privacy/, last accessed 19 September 2018
[56] See General Comment on children's rights in relation to the digital environment https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx, last accessed 6 February 2020
[57] See https://inforrm.org/2020/02/06/protecting-children-online-content-regulation-age-verification-and-latest-thinking-on-industry-responsibility-mariya-stoilva/#more-44512, last accessed 6 February 2020
[58] https://inforrm.org/2020/02/06/protecting-children-online-content-regulation-age-verification-and-latest-thinking-on-industry-responsibility-mariya-stoilva/#more-44512, last accessed 6 February 2020

There are other methods available within the English legal system that may protect this type of information. As stated above, Article 8 General Data Protection Regulation requires that parental consent be given in respect of the use of children's information and various restrictions apply. However, whilst data protection has in the past been heralded as a new weapon in privacy cases[59], it is questionable whether claims under data protection legislation offer tangible advantages over a claim for misuse of private information. In the famous misuse of private information case of *Campbell*[60], for example, whilst Morland J found that an award under Section 13 Data Protection Act (DPA) was available, a full analysis of exactly why this should be the case failed to materialise and it is not possible to identify the actual quantification of the amount awarded under the DPA. However, it may be speculated that the level of damages under this head was "not perceived to add anything"[61], an observation consistent with the derisory nature of the award under the DPA in *Douglas*[62]. Whilst Article 8 of the General Data Protection Regulation is the most recent limb of data protection regulating child data, there are shortcomings, as detailed above. Accordingly, the focus of this article now turns to the misuse of private information in the protection of childhood and, in particular, the lengths the courts have gone to under English law in order to protect the privacy of children.

The cause of action in misuse of private information has been associated with "the protection of human autonomy and dignity — the right to control the dissemination of information about one's private life and the right to the esteem and respect of other people"[63]. A two-stage process is undertaken by the courts in respect of misuse of private information claims in which a reasonable expectation of privacy, afforded under Article 8 of the Human Rights Act, 1998, is balanced against Article 10 (which provides for an explicit right to freedom of expression[64]).

---

59 McLean, A and Mackey, C, 'Is there a law of privacy in the UK? A consideration of recent legal developments', 2007 29(9) *European Intellectual Property Review* 389, 394.
60 *Campbell v Mirror Group Newspapers Ltd* [2002] EWHC 499 (QB), [2002] EMLR 30.
61 McLean, A and Mackey, C, 'Is there a law of privacy in the UK? A consideration of recent legal developments', 2007 29(9) *European Intellectual Property Review* 389, 394.
62 *Douglas v Hello! Ltd* [2003] EWHC 2629 (Ch), [2004] EMLR 2. The claimants were awarded £50 each for their claims under the DPA.
63 *Campbell v Mirror Group Newspapers Ltd* [2004] UKHL 22, [2004] 2 AC 457 [51]
64 *Campbell v Mirror Group Newspapers Ltd* [2004] UKHL 22, [2004] 2 AC 457 [12].

Whilst it must be stipulated that a child does not automatically have a reasonable expectation of privacy[65], there have been several cases in which the protection afforded to a child may be seen to be at the forefront of judicial thinking.

In *Murray*[66], for example, the key issue was whether the publication of unauthorised photographs of the infant son of author J K Rowling, in a public street, breached the child's Article 8 rights[67]. On appeal, the principal question that the Court of Appeal had to consider was whether a child was afforded a "reasonable expectation of privacy" in relation to photographs taken in a public place. On the face of it, *Murray* concerns issues very similar to those contained in *von Hannover (no. 1)* and the Court of Appeal ultimately came out in favour of the child – making this the first time in the UK that publication of a photo showing a child carrying out an everyday activity was deemed to be an invasion of privacy, Clarke MR holding that the law should protect children from intrusive media attention[68] and that the judge, at first instance, had failed to give due significance to the age of the claimant, or to the fact that the action was not brought by the claimant's parents[69].

It has been argued that the ruling effectively means that all children (whether they have famous parents or not) can now object to the publication of photographs of them taken in public places[70]. However, this is to be questioned. Whilst *Murray* does confirm that childhood privacy is capable of being safeguarded under English privacy law, the case also arguably confirms that a child will not have any guarantee of privacy. To hold that a claimant, be they a child or not, has a reasonable expectation of privacy is only the precursor to the ultimate balancing of rights, as *Campbell* attests.

---

[65] *Weller v Associated Newspapers* [2015] EWCA Civ 1176; *AAA (by her litigation friend) v Associated Newspapers Limited* [2013] EWCA Civ 554; *Murray v Big Pictures (UK) Limited* [2008] EWCA Civ 446.
[66] *Murray (by his litigation friends) v Express Newspapers plc [2008] EWCA Civ 446, [2009] Ch. 481*
[67] The claimant had been unsuccessful at first instance : see *Murray (by his litigation friends) v Express Newspapers plc* [2007] EWHC 1908 (Ch), [2007] EMLR 22.
[68] *Murray (by his litigation friends) v Express Newspapers plc* [2008] EWCA Civ 446, [2009] Ch. 481 [57].
[69] *ibid* [13] and [45].
[70] McLean, A and Mackey, C, 'Case Comment : *Mosley v News Group Newspapers Ltd*: how sadomasochism changed the face of privacy law: a consideration of the Max Mosley case and other recent developments in privacy law in England and Wales' (2010) 32(2) *European Intellectual Property Review* 77, 85.

Nonetheless, in *Rocknroll v News Group Newspapers*[71] the court was similarly swayed to grant an interim injunction to the claimant husband of the actress Kate Winslet preventing the publication of a photograph, the court considering that the risk to Miss Winslet's children "could be seriously damaging"[72]. Further, in *Weller v Associated Newspapers Ltd*, the unauthorised online publication of photographs of a celebrity's children amounted to misuse of private information[73]. As a general principle of law, in *ETK v News Group Newspapers*[74], the Court of Appeal indicated that, whilst *"the interests of affected children cannot be treated as a trump card"*[75], where children were involved, the court had a duty to treat the best interests of children as paramount when making any decision concerning them.

This is a very interesting observation. All the cases referred to above share a unifying theme : complained-of photographs. The *Weller* case, in particular, highlighted the "unique characteristics"[76] of a photograph in the context of children and it has long been established under English law that "special considerations attach to photographs in the field of privacy … As a means of invading privacy, a photograph is particularly intrusive"[77]. Reiterating this stance, The European Court of Human Rights has found that "a person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers"[78]. What is the position then if the privacy infringement does not relate to a photograph but to voice / play data? Would a court be so forthcoming in finding in favour of misuse of private information? Since someone's physical image / photograph can be copied by someone else, so can their voice be mimicked.

Voice is a unique aspect of a person's biographical data and audio files of a child's voice are considered to represent personal information under data protection law. However, interestingly, it appears that the presence of voice conversations can lower an expectation of privacy in the context of a child. For example, in *AAA v Associated*

[71] *Rocknroll v News Group Newspapers Ltd* [2013] EWHC 24 (Ch).
[72] ibid [36].
[73] *Weller v Associated Newspapers Ltd* [2014] EWHC 1163 (QB); [2014] E.M.L.R. 24 (QBD)
[74] *ETK v News Group Newspapers Limited* [2011] EWCA Civ 439, [2011] 1 WLR 1827.
[75] ibid [19].
[76] *Weller v Associated Newspapers Ltd* [2014] EWHC 1163 (QB); [2014] E.M.L.R. 24 (QBD)
[77] *Douglas v Hello! (No.3) [2005] EWCA Civ 595* at [44].
[78] *Reklos v Greece* (1234/05) [2009] E.M.L.R. 16.

Newspapers Ltd.[79] the expectation was lowered by conversations which had taken place between the claimant's mother and others[80]. Does this mean, in particular that children should be seen and not heard? Whilst there is little support for this stance, why is there privacy protection in respect of a photograph of a child but a less than robust safeguard of the captured voice? Moreover, would the innocent nature of play data be construed by the courts as trivial, being "uninhibited, casual and ill thought out"[81]? Moreover, if construed in this way, there is uncertainty over whether play data would pass the reasonable expectations threshold and no clear rules have been enunciated by the courts which clarify how trivial information should be evaluated.

Unless the play data is unidentifiable, a preferred approach would be to treat a child's play data as a private matter and their voice a "unique characteristic" of the child in the same way that a photograph was in *Weller*. However, this is not without its problems. Assuming that voice / play data would be afforded the same treatment as photographic data, the first step would be for a reasonable expectation of privacy to be made out. Moreham and Warby suggest that *the reasonable expectation of privacy test can be seen, at least in part, as shorthand for whether, in a given situation, the protection of privacy is consistent with prevailing social norms. ... if applied appropriately, the reasonable expectation of privacy test allows courts to ask… whether the scenario was one in which there was or should be an objectively recognised social norm that privacy should be respected*[82]. This is where the situation becomes complicated. How will a court deal with the data collected by Smart toys, given that social norms may become rewritten with this technology? How will courts go about determining what the

[79] *AAA v Associated Newspapers Ltd* [2012] EWHC 2103 (QB).
[80] Although note that the publication of a photograph of the child was still not justified. See https://login.westlaw.co.uk/maf/wluk/app/document?&srguid=i0ad832f200000165e723f8043ef75c7c&docguid=I93FC5C00EA6611E39B96B7C6DF412BB7&hitguid=I93FC5C00EA6611E39B96B7C6DF412BB7&rank=1&spos=1&epos=1&td=1463&crumb-action=append&context=31&resolvein=true, last accessed 17 September 2018.
[81] *Smith v ADVFN Plc* [2008] EWHC 1797 (QB) [14].
[82] Nicole Moreham and Sir Mark Warby (eds), *Tugendhat and Christie: The Law of Privacy and the Media (* 3 rd edn, 2016), 49.

appropriate norm is in this context[83]. How will they balance parental expectations that a child's information should be considered private[84]?

At this point, it is important to challenge certain notions around childhood privacy. On the one hand, it has been argued that "privacy is dead'[85] and that technological advancement has "made it either impossible or extremely costly for individuals to protect the same level of privacy that was once enjoyed"[86]. Accordingly, since smart toys pose a serious threat to childhood privacy, it may be argued that childhood privacy is harder to protect. Discussions on smart toys certainly suggest that the collection of data from children eats away at their privacy and is, by definition, problematic. Yet, are they in a way like police body cameras? These can both infringe privacy, but may also exonerate suspects and even hold police accountable. Therefore, it is the switching off of such cameras that has become the problem rather than their presence. This raises the question of whether it is even clear that children's right to privacy is a social good given that it is arguable that the use of privacy in relation to children has actually also caused them harm (child abuse, institutional sex abuse etc) because the associated lack of data or records has operated to protect adult perpetrators. Adult perpetrators can, ofcourse, come from a variety of sources. So, could we imagine a smart toy (the next version of the My Friend Cayla doll perhaps) that is programmed to pick up concerns raised by the child about their treatment by adults – be they parents or guardians, for example, and alert the authorities? In effect, this raises the same debates about state intervention in family life that child protection laws do. Thus, the issue may not be whether smart toys should collect data from children, but rather *how* the private corporation's collection of the data should be treated.. The German approach to smart

---

[83] See https://login.westlaw.co.uk/maf/wluk/app/document?&srguid=i0ad832f100000165e736c06d4c26c0c9&docguid=I14C818D01B5811E89FB4C99500526EEA&hitguid=I14C818D01B5811E89FB4C99500526EEA&rank=12&spos=12&epos=12&td=1463&crumb-action=append&context=35&resolvein=true, last accessed 17 September 2018.

[84] Leo Kelion, "Posting children's photos on social media divides nation' BBC, 3 August 2017 http://www.bbc.co.uk/news/technology-40804041, last accessed 17 September 2018.

[85] Alex Preston, "The Death of Privacy,' *The Observer,* 3 August 2014 https://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston; Jo Glanville, "Privacy is Dead! Long live privacy' (Sage Publications, 2011); Bobbie Johnson, "Privacy no longer a social norm, says Facebook founder,' *The Guardian,* 11 January 2010. https://www.theguardian.com/technology/2010/jan/11/facebook-privacy; Business Wire, "Digital Birth: Welcome to the Online World' http://www.businesswire.com/news/home/20101006006722/en/Digital-Birth-Online-World, last accessed 17 September 2018.

[86] Gavison R, 'Privacy and the limits of the law', (1980) 89 *Yale Law Journal* 421, in Schoeman, F (ed), *Philosophical Dimensions of Privacy : An Anthology* (Cambridge University Press, 1984) 376.

dolls provides a good example here. In Germany, these toys are cast as spies – but who are they spying for? The corporation? The state? The parents? The child? This is essentially akin to the cameras used to spy on nannies – in so far as these devices are able to pick up abuse that may then be prosecuted and this serves to protect children's rights. Why, then, have smart toys been cast as clear villains? Is it that parents fear intrusion into their domain? The smart toys narrative still sees children as vulnerable and requiring parents to make decisions for them? Whilst the GDPR discussion on lowering the age threshold accords to children some capacity to make their own decisions, the smart toys narrative still sees children as vulnerable and requiring parents to make decisions for them. But it is at least arguable that this a complex and contested area and that there are clear contradictions in the law that have been mentioned above.

There is therefore a conundrum : the protection of a child's right to privacy versus parental controls and expectations of control, especially where those expectations actually expose parental weakness (or worse)

CONCLUSION

In conclusion, debates about control and surveillance of play data are not going to go away. The impact of technology from a number of perspectives on childhood raises an assortment of concerns which could put the privacy and safety of children at risk. Risks for children's rights to privacy are one of the most visible and immediate consequences[87], as this article has highlighted. Essentially, the problem is that play data / voice recordings can be stored and used for a variety of purposes beyond providing for the toys' functionality[88]. This exposes problems in terms of data and privacy protection and this means that, in addition to the child's online safety, data protection and privacy issues should be considered as a primary concern for shoppers buying smart toys.

We are still facing important questions, particularly in relation to what shape online safety regulation should take, and where it should come from. As far as the reach of

[87] Stephane Chaudron et al, 'Kaleidoscope on the Internet of Toys' [2017] JRC Technical Reports, page 18 <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC105061/jrc105061_final_online.pdf> last accessed 14 February 2020.
[88] https://mobile.nytimes.com/2017/02/17/technology/cayla-talking-doll-hackers.html?emc=edit_th_20170219&nl=todaysheadlines&nlid=55059608&referer=

the law is concerned, whilst protection is theoretically available under both data protection and misuse of privacy avenues, the fact remains that children's childhoods are potentially at risk from a variety of sources and the very regulation that serves to protect childhoods could infact be exposing it to additional dangers. Therefore this article has raised questions about whether the current protections available produce adverse consequences that need to be addressed. In particular, although the GDPR has ushered in the largest overhaul in data protection rules Europe has seen in twenty years, the use of parental consent in the legislation produces unexpected results which are not as palatable as first anticipated.

Legislators when designing the GDPR arguably failed to consider that children require rights separate from their parents in some situations. While most parents will have the best intentions in mind for their child, others may not, and that must be taken into consideration. The approach of legislators when balancing protection for children with their human rights must be to create policies that allow opportunities to access information online with the need to minimise exposure to safety and privacy risks. In this way, smart toys can represent a safe form of technology for child users, but they must be accompanied by detailed legislation that takes into account the unexpected outcomes that the current data protection regime has nourished.