2017

Discursive constructions of the internet of toys

Lelia Green
Edith Cowan University

Donell Holloway
Edith Cowan University

Discursive constructions of the Internet of Toys

Lelia Green, Edith Cowan University, l.green@ecu.edu.au

Donell Holloway, Edith Cowan University, donell.holloway@ecu.edu.au

Abstract

The Internet of Toys (IoToys) refers to the small subset of the Internet of Things often marketed to children and their caregivers as smart toys. These toys include many of the affordances of screen-based, networked technologies, packaged as children's everyday playthings. Thus, Hello Barbie uses voice recognition and cloud-based computing combined with artificial intelligence procedures to craft meaningful responses to children's statements and engage them in quasi-naturalistic conversation. Other IoToys also include image recognition and geo-locational data collection. Such toys can also be constructed in different ways that represent the perspectives of the speaker and circumstances of use. Thus Germany's Federal Network Agency announced in February that it classified the My Friend Cayla doll (a competitor to Barbie) as an 'illegal espionage apparatus' because 'under German law it is illegal to manufacture, sell or possess surveillance devices disguised as another object'. The IoToys facilitates both commercial relations and income streams for the manufacturers and/or associated organisations, such as marketing agencies, software providers and voice analytics services. These streams of income can include advertising to children through the connected toy, the collection, analysis and monetisation of children's data and the sale of the toy itself. Buying the toy also involves long-term contractual agreements that transfer legal responsibility for the collection, analysis and distribution of children's data onto their parents. This effectively gives commercial entities the authority to continue and conceivably expand upon data-collecting and data-sharing procedures. This article analyses the discursive construction of the future IoToys using textual analysis of media resources that provide stakeholder perspectives on this emerging field. It argues that, given their status as an emerging category of human–computer interaction devices, objects that can be classified as part of the IoToys currently occupy a controversial and contested media industries space, raising many regulatory and policy questions that children themselves are not equipped to consider or take into account.

Keywords: children's rights; discourse analysis; Internet of Toys; revenue streams; surveillance; privacy

---

Introduction

The Internet of Toys (IoToys) is an emergent category of goods marketed to parents as smart toys and to children as fun. These items offer children an augmented play experience in that smart toys are connected via wi-fi to cloud computing technologies and incorporate a range of hi-tech features such as image-recognition software, geo-location tagging and movement sensors. A brief survey of the range of stakeholders in the IoToys industry ecosystem indicates the vested interests at play:

- toy manufacturers
- software and hardware developers
- privacy and security specialists
- commercial/advertiser interests
- policy-makers and regulators
- consumer and advocacy groups
- media commentators
- children
- parents.

Given the many stakeholders implicated in this emerging technological and commercial space, it is unsurprising that the discursive construction of the IoToys is highly contested.

This article analyses multiple stakeholder positions on IoToys development, and examines the manner by which different stakeholders construct the materiality of internet-connected toys: as data-collecting technologies and enterprises that threaten children's data privacy and security; as positive, educational and fun products for children; as sophisticated AI technologies at the forefront of technological innovation; as hackable, insecure technologies that may be hijacked by others and threaten individual children's safety; as platforms for further commercial marketing to children; as controversial, paradigm-shifting technologies worthy of news coverage; or as nothing of particular concern, to be responded to in a low-key manner.

The authors argue that, despite these diverse discursive constructions all vying against each other, the two most dominant voices are both commercially based: the toy companies themselves and their associated IT support services; and/or privacy and security entrepreneurial individuals or companies. These commercial entities use contrasting ways to make parents responsible for their child's activities: the toy companies and associated support services make parents responsible for the social and educational progress and behaviour of their children; and privacy and security entrepreneurs make parents responsible for their child's online safety. Children's rights to participation and protection, on the other hand, are embedded in lesser discourses taken on by consumer groups in Europe and the United States that have contributed to debate around the introduction of connected toys, as well as the emergence of regulatory and policy investigations and discussions in Europe and North America. However, little movement in this space is occurring in Australia.

Methodology

This article adopts a 'political economy of communication' framework to explore 'the study of the social relations, especially the power relations, that mutually constitute the production, distribution, and consumption of resources' (Mosco, 2009, p. 25). In this case, the resources considered were media resources that were available in the general public sphere applicable to the IoToys during the period 15 November 2016 to 10 January 2017, as well as an augmented purposive sampling of publicly available discourses in order to fully analyse the nine stakeholder discourses. The original sampling involved 203 commentaries, and 47 advertisements were collected from public media in twelve countries: Australia, Austria, Finland, Germany, Italy, Lithuania, Malta, Portugal, Romania, Serbia, Slovenia and Spain. These commentaries and ads were then analysed and coded for outlet type, toy type, positive or negative statements, centrality of children within the discourse, risks mentioned, opportunities cited, the origins of the commentary and the voices being used within the commentary: parents, children, toy industry, Internet industry, government, institutions, NGOs, consumer groups, researchers, manufacturers, internet security experts/companies and so on. The findings and discussion around this analyses were published in 2017 and comprised discussions about the parental responsibilisation discourses evident within the public commentaries, the gendered nature of connected toys, the risks and benefits of connected toys evident in the commentaries, and global and local insights connected with the development and take-up of the toys (Mascheroni & Holloway, 2017).

As can be appreciated, different elements of the nine sets of stakeholders identified above are differently invested in the production, distribution and consumption of IoToys-related media accessible via the general public sphere. Furthermore, two perspectives were almost entirely absent from the data collected: parents' and children's voices – apart from cases where parents were also security experts, or toy manufacturers. Given this absence of general comments representing these stakeholder categories, they will not be considered further in this article; however, they remain a critical absence in the discursive record. It should be noted here that there is, however, an emerging children's public sphere where IoToys are presented and played with, with YouTube now having many 'unboxing' and 'play with me' videos with connected toys.

The analysis in this article utilises the data gathered above as a starting point for inquiry; however, the analysis does not seek to quantify different stakeholder perspectives, or an investigation of relative 'share of voice' (Hansen & Christensen, 2005; Macnamara, 2005, p. 21). The originally collected media texts were augmented by a purposive search from newspapers, magazines, blogs, product reviews, parenting forums, mummy bloggers, parenting magazines and so on, to further capture the perspectives of stakeholders who were under-represented in the initial dataset, even though everyday parents and children remained under-represented. Using constant comparative analysis (Fram, 2013) to evaluate each stakeholder's constructions of the IoToys, this article explores the range of speaking positions and discourses through which the political economy of the IoToys is framed within the general public sphere.

Selected media texts were further analysed using critical discourse analysis (Fairclough, 1992, 1995) to establish their contribution to the contested construction of the IoToys.

This article has a range of limitations. The first is that this analysis – as with all discourse analysis – does not examine or quantify the impact of any of the public discourses analysed on their audiences. On the other hand, the media do play a role in the amplification of concern and risk via publicly available commentary (Thiesse, 2007). They then also play a 'significant role in forming and shaping risk scenarios' (Slettemeås, 2009, pp. 230–1) to inform design, policy and the public. The second limitation is that the sample of materials analysed is effectively one of convenience, since the core of the dataset had already been collected. The purpose of this article, however, is the identification of the diversity in discursive constructions relating to this topic area, rather than an assessment of proportionality for each position (Mascheroni & Holloway, 2017). In this circumstance, a convenience sample underpinning an established contribution to the field (Holloway & Green, 2016), augmented by a purposive search to address identified gaps and absences, constitutes the data for a critical investigation. As this investigation relies on accessible media texts, it aims to cover examples of constructions of the IoToys attributed to each of the sets of stakeholders identified. It then uses those materials to interrogate the possible existence of further groups of stakeholders and/or missing voices, such as parents and children.

This investigation will analyse the dataset established, addressing the following research question:

> What does a critical discourse analysis of media commentary relating to the IoToys tell us about the variety of speaking positions occupied by stakeholders, and the discursive constructions of this set of ICT devices?

Children's play and the IoToys

Although there is a general absence of parent, family, child and community discussion of the IoToys in the general public sphere, there is work around new and emerging digital toys that indicates the need for ethnographic research with a particular IoToys focus. Significant scholarly attention has already been paid to digital toys and hybrid play, and some of that work will be considered briefly here to create a context for the commentary that constitutes the political economy of communication in the area of IoToys.

Marsh and colleagues (2017) firmly locate the growing digital competencies of even very young children (aged two to four years) within their family context. Their study of four families with young children indicated the 'children were immersed in a range of multimedia, multimodal practices which involved extensive engagement with other family members who scaffolded their learning and delighted in the children's technological capabilities' (2017, p. 47). Part of this 'delight' in children's technological and digital prowess reflects generally held beliefs that:

> It is necessary but no longer sufficient for children to develop competence in relation to written texts; they also need to be able to engage successfully with multimodal, multimedia texts if they are to acquire the range of skills, knowledge and understanding necessary to navigate the knowledge economy of the

21st century. (Marsh et al., 2017, p. 48, referencing Lankshear & Knobel, 2011).

This, then, is the high-stakes context in which parental investment in digital play experiences, and internet-connected toys, takes place.

The IoToys is one specific aspect of children's digital technology use, and the younger the child, the more reliant they are on parental guidance to avoid behaviours that include risks of unexpected or unanticipated consequences (such as an early years digital footprint, or monetisation of a child's online data). Jayemanne and Nanson (2016, p. 135) explore the concept of younger children's digital dexterity in the context of touchscreen devices via 'themes of imagination, encounter, and mobilization', where 'how media are imagined is situated in relation to interface studies, debates about the naturalness of NUI [natural user interfaces, … and how] mobile media and gestural interfaces influence children's play, education and development'. The facilitation of children's encounters with such touchscreen technologies is a specific aspect of 'technology domestication within the home', as Marsh and colleagues (2017, p. 135), demonstrate. Finally, Jayemanne and Nanson (2016, p. 147, citing Lupton, 2013) discuss mobilisation in terms of parental mediation and the 'ongoing process of interembodiment', 'to designate the communicative circuit between parent, child and mobile touch-screen device'. These aspects of imagination, encounter and mobilisation are arguably of even greater importance where there is no necessary computer screen, and where an internet-connected toy might be activated by voice-recognition technology or movement sensors. In many IoToys, the digital aspects of the technology, and its connection to the internet, are deliberately obscured so that the toy seems to conform to conventional analogue expectations of (say) a teddy bear or a doll. This can have privacy and regulatory implications, such as those faced by the My Friend Cayla doll (BBC, 2017; Walker, 2017), and children's smart watches (Singleton, 2017; Wakefield, 2017) in Germany.

Tyni and colleagues (2016) examine what they term 'hybrid playful experiences: playing between material and digital', noting that 'the dynamic and smart capabilities of computer software, sensors and networks provide, at least in principle, limitless opportunities for transforming the mute physical object into something that can sense, react and invite to rich, playful interactions' (2016, p. 16). Noting the 'constantly advancing frontier of playful hybrid products, environments and associated services' Tyni and colleagues (2016, p. 16) go on to argue that it is 'becoming difficult to detect miniature chips, power sources and printed circuitry embedded in various, seemingly common, everyday objects'. As these authors note of 'smart toys', 'using an online connection or a smartphone as an element of the product experience allows users to modify and rejuvenate their experiences … A shared characteristic between most smart toys is that they can be updated, ideally providing prolonged usage. This, subsequently, can be seen [as] turning the toys into evolving services' (2016, p. 53). For the various IoToys stakeholders, the capacity of a toy to offer a range of novel and evolving experiences means that the toy can change and grow with its owner, or in line with new opportunities to monetise the product as these emerge.

The commercial aspects of the IoToys include the physical sale of the toy itself and the requirements of its connectability (such as wireless internet and, potentially, a

subscription to a package of features); the sale of the data generated by child users to other commercial interests; and the commercialisation of the messages conveyed to the child by the IoToy communication system (Holloway & Green, 2016). Grimes (2015, p. 110), examining the commercialisation aspects of comparatively well-established children's virtual worlds, argues that:

> These games are designed to mobilize virtual economies for real money transaction and self-promotion, utilizing game mechanics, virtual items, and other features for various forms of branding and third-party advertising strategies … such processes work to mobilize players' affective labor, while concurrently limiting potentially important opportunities for participation, communication, access, and cultural rights, such as freedom of speech.

Giddings (2017, p. 59) makes a similar point concerning Pokémon Go:

> the workings of imagination in children's lives have always populated mundane experience with nonactual actions and characters, and these processes have been mechanized and monetized by commercial children's culture over decades, not least in the transmedia system of Pokémon itself.

As can be seen, critical commentators such as Grimes (2015) and Giddings (2017) have carefully considered and analysed the ways in which a seemingly innocent play experience delivers value to toy manufacturers and ancillary service providers. Such monetisation of leisure, play and 'educational' experiences (as with app-enabled products) is rarely overt or explicitly consented to. Indeed, parents might believe that regulations expressly forbid such commercialisation of children's data or the monetisation of children's 'affective labour' – that is, 'where social relations and peer dynamics are reported to generate an enormous amount of surplus value' (Grimes 2015, p. 126). Given that such matters are opaque in the contractual communication between toy purveyors and parents or other bill-payers, they are rarely appreciated at all by the children themselves.

Acknowledging these complications, one way forward is to focus on a children's rights perspective, in order to make children's rights central to:

> children's formal and informal learning; health and wellbeing; literacy; civic and/or political participation; play and recreation; identity; belonging; peer, family and intergenerational relationships; individual and community resilience; and consumer practices (Livingstone & Third, 2017, p. 666, citing Swist et al., 2015).

This rights-based perspective is generally absent from the general public sphere discussions of the IoToys, except in discourse promoted and circulated by consumer and advocacy groups, and repeated in media commentary. In other words, this discursive position is recognised largely by its absence.

The discussion now turns to consideration of the various discourses and speaking positions identified in the analysis of perspectives readily accessible via the general public sphere.

Findings

Toy manufacturers

Since toy manufacturers are the key instigators of goods and services for the IoToys, their discursive currency tends to be positive and aspirational. Thus Mattel says of its flagship IoToy product Hello Barbie that it is the doll 'that converses with kids, remembers things they say, and recalls details later' (Newman, 2015). For busy, distracted parents, increasingly challenged by the recall of detail, such a product offers clear opportunities for their child to refine their verbal engagement and technology skills. Indeed, educational and techno-savvy discourses are significant elements of the manufacturers' promotion of the IoToys, with products available that support individualised child-centred learning experiences, and the early acquisition of digital skills such as coding. Programmable robots Dash and Dot, for children aged from five to eight years, are said to 'ignite curiosity and confidence while providing fun ways of learning the essential skills of collaboration, communication, and digital literacy' (Wonder Toys, n.d.); while the programming of kids-size 3D printer ThingMaker is designed to get children 'interested in design and manufacturing, as well as developing their creative skills to make their own objects' (Barrett, 2016).

Even if the manufacturer's preferred discourse is one of benefit and unproblematic enjoyment, the countervailing power relations existing in this sphere pose a challenge to the credibility of these claims. White hat hackers (Caldwell, 2013; Moini, 2017), internet security experts who work to expose vulnerabilities in IoToys products, have often disrupted the preferred manufacturers' discourse, prompting toy developers to engage in a defensive minimisation of security risks along with a public display of concerned commitment to action where required. Thus VTech (2016) constructed a dedicated site to demonstrate the seriousness it attributed to the 2015 hacking of its VTech Learning Lodge stable of products. It also closed down a range of services and took the products offline for remediation, although it was unclear what differentiated those products that were returned to the market from those that were removed permanently. According to Bogart (2016), however, the contrition was more apparent than real: VTech quietly changed its terms and conditions of service to ensure that liability for future hacks was shifted to the users of the toys. Thus the company exonerated itself from responsibility for any harm to users by introducing new consents required for consumer access.

Software and hardware developers

Toy manufacturers such as Mattel generally lack the skill set and technical infrastructure required to venture unsupported into the IoToys space. In the case of Hello Barbie, Mattel partnered with IoToy digital specialists Toytalk. These developers of software and hardware tend to be allocated the 'speaking position' when there are threats to the integrity of the product – for example, when an IoToy product has been hacked. The communicative register, 'referring to situationally defined varieties [of language]' (Biber, 1995, p. 1) in this case, is somewhat different when the speaker is a technology specialist, compared with when they are a non-tech-specialist toy manufacturer. Thus

Mattel's technology partner ToyTalk responded to one of the Hello Barbie hacks with an implied request for the cyber attackers to acknowledge that the company had exceeded the general level of security performance, even if the toy had proven vulnerable.

On behalf of ToyTalk, Martin Reddy argued that it had 'added client certificate authentication [to Hello Barbie], above and beyond what most Internet-connected devices do, as a way to deter a casual attacker' (cited in Adhikari, 2015). Here, the discourse is one of expert to expert – in effect, paying a compliment to the hacker (they're not 'casual') and asking for validation of the additional focus on security. Reddy also asserted that, even if the product security could be compromised, the impact would be limited since, according to ToyTalk, even a successful hack allows 'no access to WiFi passwords, no access to child audio data, and cannot change what the doll says' (Adhikari, 2015). In at least one instance, this ToyTalk discursive strategy seems to have worked. White hat hacker Jakubowski responded by admitting that Hello Barbie featured 'good levels of security that you don't typically see in many IoToys devices. ToyTalk has certainly taken many of the concerns and has addressed them as best as they could' (Bogart, 2015). This all-tech-friends-together tone of exchange was reinforced by ToyTalk's subsequent announcement that it was 'creating a "bug bounty" program that will reward security researchers for responsibly disclosing security vulnerabilities' (Bogart, 2015).

In other cases, the discursive register of toy manufacturers is changed to speak directly to the consumer market. Thus Bob Delprincipe, the inventor of My Friend Cayla, which he claims to be the first internet-connected doll (Wallop, 2014), marketed by UK toymaker Vivid, says of Cayla, 'She's not a search engine, she's a seven-year-old girl. There are some things she just doesn't know' [… the journalist notes that] Say the word 'crap' to the doll, and she answers: 'That's inappropriate.' Ask her where babies come from and she says: 'I don't know. You better ask your teacher."' (Wallop, 2014). Unsurprisingly, some tech hackers have taken this as an invitation to get Cayla to say some very choice words not included in the average seven-year-old girl's vocabulary (PenTestPartners, n.d.).

Privacy and security specialists

As demonstrated by this discussion of software and hardware developers' discursive interventions within the general public sphere, some privacy and security specialists gain their speaking privileges from what they do by using their technological expertise to prove their point by exploiting and publicising the technical vulnerabilities of the IoToys. For example, *SBS News* (2015) cites the alleged white hat VTech hacker's comment to online security publication *Motherboard:* 'Frankly, it makes me sick that I was able to get all this stuff'. Australian security specialist Stilgherrian (quoted in Timms, 2015) suggests that:

> We're going to see more and more of this kind of security vulnerability crop up, simply because we're getting companies, in this case it's a toy manufacturer, none of these organisations have a tradition or have the internal company infrastructure to constantly test and retest their devices

> and issue security updates for it … If we're having trouble convincing people they need to install the security updates on their phone, it's going to be a lot harder to convince them to update the software on their doll.

The 'privacy and security specialist' category can also include the inverse skills, the specialist black hat hackers who have malicious intent when compromising IoToys. This seems to be the case with the hack of CloudPet Teddy Bear, which had impacted at least 800,000 people by February 2017 (Moini, 2017). In this instance, there was no friendly inter-exchange between the hackers and the toy manufacturers or their tech partners – indeed, the hackers' aim seems to have been malicious. According to Chester (2017), 'along with the database of user names and email addresses, the hackers also had access to 2.2 million recorded messages between children speaking to their toys'. Hunt (2017) states that 'The CloudPets data was accessed many times by unauthorised parties before being deleted and then on multiple occasions, held for ransom.'

Commercial/advertiser interests

There are some indications that negative messages about the IoToys are making an impact in the marketplace and affecting the sales of these toys. Hunt (2017) points out that at the point when the CloudPets hack story was broken, the company's share price was less than 1 per cent of its previous highs, and hovering at US$0.0044 cents per share (on 22 February 2017). The discursive positions of media commentators have clear impacts in this case.

Other commercial interests, however, see an advantage to 'linked selling' and third-party advertising via the IoToys. This is the case with the suspected alliance between Disney and Genesis, the manufacturer of My Friend Cayla (Cayla suggests Disney movies to child users.) While there are no contractual relationships between the two companies, they both use voice recognition services provided by Nuance Communications – the company tasked with scripting and providing Cayla's voice conversations and voice analytics for My Doll Cayla (Mlot, 2016).

As part of the flurry of IoToys commentary that often circulates in the media alongside the Christmas present-buying season (in this case, 8 December), Roberts (2016) notes that the Electronic Privacy Information Centre (supported by the Campaign for a Commercial Free Childhood and the Center for Digital Democracy) had filed a complaint with the US Federal Trade Commission (EPIC, 2016) which alleges the following about the IoToys smart doll:

> My Friend Cayla is pre-programmed with dozens of phrases that reference Disney movies and theme parks. For example, Cayla tells children that her favorite movie is Disney's *The Little Mermaid* and her favorite song is 'Let it Go' from Disney's *Frozen*. 'Cayla also tells children she loves going to Disneyland and wants to go to Epcot in Disneyworld,' says the complaint, which says such activity amounts to a deceptive form of product placement. (Roberts, 2016)

It would seem that this commercial alliance is post hoc, since on the initial release of the toy it was noted that Cayla's favourite film was '*The Sound of Music* – chosen so that there are no licensing issues with a Disney film' (Wallop, 2014). This allegation of product placement, and the discursive content that speaking IoToys communicate to their young owners, indicates that manufacturers are diversifying their income streams from these products. Not only are they providing consumer goods for children, they are providing commentary on behalf of commercial organisations and 'it is becoming more and more common for smart toys to store and sell data about how they are played with' (Tait, 2016). In general, however, the voices of commercial interests invested in the IoToys – apart from the companies that make, market and service the products themselves – are absent from the public debate.

Policy-makers and regulators

Despite the fact that the Federal Trade Commission and the European Union have yet to rule on law suits filed against IoToys manufacturers, the German Federal Network Agency has actively banned My Friend Cayla as a 'concealed transmitting device' (BBC, 2017) and an 'illegal espionage apparatus' (Walker, 2017), both of which are prohibited under Germany's strict privacy and anti-surveillance laws. The actions of the Federal Network Agency reflect Germany's recent history, in which surveillance is a 'particularly sensitive issue in Germany where East Germany's Stasi secret police and the Nazi era Gestapo kept a close watch on the population' (*The Guardian*, 2017). Not surprisingly, the agency has more recently banned the sale of children's smart watches because they can be used to spy on others – for example parents listening in on their children's teachers during class time (*The Guardian*, 2017). In addition to the concerns of this German agency, the BBC reports that Vera Jourová, the EU's Commissioner for Justice, Consumers and Gender Equality, stated, 'I'm worried about the impact of connected dolls on children's privacy and safety' (BBC, 2017).

In Australia, the eSafety Commissioner has information about 'Smart toys', 'Connected Toys' and 'Robotic Toys' on its eSafety gift guide website (eSafety, n.d.), and it has also issued occasional press commentary about the Australian impact of some of the better publicised hacks. Thus, the then Children's eSafety Commissioner Alastair MacGibbon said of the VTech hack that 'the theft of data relating to children' added 'a degree of injustice' to the breach. 'Why are we collecting this information to start with? If you don't collect it, you can't lose it?' (SBS, 2015). At present, there is no regulatory response stronger than consumer information on the Commission's website, implying a low-key reactive discursive response rather than the more proactive stance that might be expected of an organisation that advocates for children's e-safety rights.

Consumer and advocacy groups

While privacy and security experts are increasingly attempting to engage in detailed exchanges with policy-makers and regulators around these different issues, consumer and advocacy groups in the United States and Europe have recently carried out a carefully orchestrated publicity campaign regarding internet-connected toys. In the lead-up to Christmas 2016, a collaboration of privacy and consumer groups from the

United States and Europe took legal action by filing a series of formal complaints with the European Commission (EC), the International Consumer Protection and Enforcement Network and product safety authorities in Norway, Belgium, France and the Netherlands (Europe) and the Federal Trade Commission (US). These complaints were based on research carried out by the Norwegian Consumer Council into safety and privacy issues related to Genesis' toys, Cayla and iQue, as well as Mattel's Hello Barbie. Their report *Toyfail* 'revealed serious risks to, and a lack of understanding of, children's rights to privacy and security' (BEUC, 2016).

This campaign was coordinated by the Electronic Privacy Information Centre (EPIC), the Campaign for a Commercial Free Childhood (CCFC), the Centre for Digital Democracy (CDD), and Consumers Union (in the US) and by Forbrukerradet, the Norwegian arm of the European Consumer Organisation BEUC (an umbrella organization for 43 European consumer advocacy groups) in Europe (BEUC, 2016; Keller & Hackman, 2016). It has also successfully challenged regulatory authorities across the Atlantic to pay attention to the policy and regulatory needs of this emerging market, particularly in terms of what needs to be done with regards to policy, practice and parenting advice.

Although the Federal Trade Commission in the US is yet to rule on the EPIC suit (EPIC, 2017), a Congressional Investigation is taking place led by Senator Edward Markey (EPIC, 2016) and the EC recently instigated a joint workshop with Member State authorities to ensure that manufacturers and suppliers of internet-connected toys and apps conformed to EU law (EU, 2017). Commissioner for Justice, Consumers and Gender Equity Vera Jourová said:

> While technological developments and new digital products are enriching our daily lives, EU citizens rightly expect that their products are, first of all, safe. In particular, when it comes to the most vulnerable. For example, more and more children are playing with connected toys. Their parents must be able to rest assured that these toys are safe for them to play with and that their privacy is respected' (EU, 2017).

Media commentators

The media are a well-established player in the political economy of communication, with an accepted role in reporting the very best of ground-breaking, paradigm-shifting innovative advances alongside the very worst of privacy-invading, security-breaching assaults upon the individual and the family. These accounts might even refer to the same product, in the same news cycle. The overall aim of most mainstream media – but especially media that are commercially driven – is to gain attention and traction through clicks and ratings. Moderate discussion with a nuanced argument has rarely succeeded in achieving this. Instead, the media may sometimes play a polarising role (Cohen, 2002).

At the same time, the media serve the role of being the primary provider of a speaking platform for diverse interest groups, including those discussed previously, and currently act as a kind of archival record allowing for investigations such as this one. Thus the media have less of a speaking position in their own right on a subject such as

the IoToys, and play more of an amplification or muffling role in permitting some voices and discursive positions to be promoted while others are muffled, suppressed or not sought out.

Parents, children, families and community

These voices have yet to emerge clearly within the mediated general public sphere, apart from token interviews and responses quoted by the media to establish a human face for a policy discussion. Indeed, a close encounter with the general public sphere materials concerning the IoToys indicates that parents are more spoken to and about than speaking themselves. For example, Hunt warns that:

> Circling back to the parents' position for a moment, you must assume data like this will end up in other people's hands. Whether it's the Cayla doll, the Barbie, the VTech tablets or the CloudPets, assume breach. It only takes one little mistake on behalf of the data custodian – such as misconfiguring the database security – and every single piece of data they hold on you and your family can be in the public domain in mere minutes. (Hunt, 2017)

While it is likely that some of the featured specialist commentators, such as white hat hackers, have a further identity as 'parent' and this may explain part of their motivation for intervening in this space, that personal perspective is rarely made clear in the constructions around specialists' discourse. Thus the speaking position for parents is mainly confined to individual consumer acts of acquiescence (the smart toy gets purchased) or resistance (the home becomes a smart toy-free zone).

Although children's rights in this arena (Holloway & Green, 2016) have motivated a range of media and expert commentary (e.g. Livingstone & Third, 2017), some regulator-driven intervention in Germany (BBC, 2017) and an EPIC submission to the US Federal Trade Commission (EPIC, 2016), children themselves are generally constructed as too young to participate in debates such as this one. Indeed, parents are presented as worryingly ignorant from the experts' point of view: 'What worries me is that it's hard for the parent to know' (Walsh, 2017). Newman (2015) cites Angela Campbell, who works at Georgetown University's Center on Privacy and Technology, and who was interviewed by the *Washington Post*, as saying, 'If I had a young child, I would be very concerned that my child's intimate conversations with her doll were being recorded and analyzed.' The thing about young children is that they are not old enough to know better. In these circumstances, children are most likely to be talking to their IoToys, but least likely to be critically evaluating them.

Comment by and between parents, children, families and communities is likely to be circulating informally as a result of these parties' considerations of the various discussions in the general public sphere. The lack of such voices in the general public sphere, incorporating the attitudes and considerations of parents and children, demonstrates the need for ethnographic work in this area to capture and circulate everyday considered reflection upon the lived experience of, engagement with and concerns regarding IoToys. In addition to this, some children seem to be promoting IoToys through YouTube 'unboxing' and 'let's play' vlogs, either as part of professional YouTube channels or as part

of a more amateurish imitations of these professional ads. This children's public sphere (YouTube) also requires investigation and discussion. As a quasi-marketing practice, these 'unboxing' and 'let's play' videos engage children both as producers (child vloggers) and consumers (advertising targets) in mixing advertisements with content – something not usually allowed in children's television regulation.

Discussion and conclusion

The research question motivating this article is:

> What does a critical discourse analysis of media commentary relating to the IoToys tell us about the variety of speaking positions occupied by stakeholders, and the discursive constructions of this set of ICT devices?

The analysis here finds that there is a range of claimed and demonstrated 'power' at play in this space, complemented by differently constructed speaking positions. The main sources of power harnessed in this debate are commercial power, technological power, and consumer and advocacy groups. There is some evidence of the potential of regulatory power, although this is mainly latent at present.

Commercial players are implicated through the construction and marketing of IoToys, in alliance with their tech partners. Secondary commercial players include 'product placement' organisations that get smart toys to introduce targeted products in their discourse with children, and those organisations interested in acquiring information around how children play with and talk to smart toys, and the data sets that these activities create. To some extent, this commercial power is countered by the technological power wielded by white and black hat hackers. The aim of these individuals is to exploit weaknesses in the privacy and security systems of IoToys to reveal vulnerabilities on the one hand and their own skills on the other. Many of these tech experts run their own companies, and associated blogs or newsletters, so these actions offer multiple benefits in terms of promoting them and their work while, they would argue, making the internet safer for young children.

Consumer and advocacy groups in this space are often motivated by privacy and security concerns, but generally seem more willing to take a stand than the organisations that have been funded specifically to intervene on citizens' behalf (or, in the case of children, on behalf of minors). The groups across Europe and the United States concerned with these issues have carried out relatively successful publicity campaigns. However, with the comparatively limited resources afforded to these groups, as well as the multiple issues on which they may be campaigning, it is not yet clear whether this momentum can be sustained.

Strong regulatory and policy advances are so far lacking. The only clear exception to this general rule is in Germany, where the regulator has made a clear statement about IoToys, My Friend Cayla and children's smart watches. Apart from these two instances, regulators and government bodies seem unwilling to intervene in this space, prompting non-government advocates and consumer groups to expand their efforts as a means of filling the vacuum, trying to effect regulatory engagement. All these various actions and

reactions feed into the media's search for hot-button topics that constitute communicative power through the provision of rich, deep material for comment and controversy.

As for the discursive constructions on display, the dominant voice across media platforms is a commercial one. In addition to the IoToy product and its advertising – noting that some media organisations will be inhibited from comment because advertising revenues may be impacted – these commercial interests are looking for multiple ways to monetise their IoToy products. The terms and conditions signed by the consumer may have no indication that what they are agreeing to includes product placement by some of the biggest names in children's culture. Further, toy organisations are not explicit about capturing, for example, the verbal records of children's hopes, questions and confidences, retaining the rights to on-sell these data where possible. Because the manifestation of the IoToys discussed here occurs within the context of a free-market economy, commercial discourses are generally taken for granted: they are the continuous background to the other conversations because society is structured to support and profit from their existence.

Opposing this general background noise of business as usual, the tech hackers, the media, and advocacy and consumer groups all vie for their share of voice, for their own reasons. Those reasons might be so complex that 'raising my own profile' becomes translated in the speaker's mind as 'making a difference'. Whatever the underlying discursive motivator(s), in the absence of these voices little would be happening to challenge the dominant commercial discourse, which peaks every year around Christmas. Even with the disparate voices of hackers, media and advocates, there is little evidence of intervention on the part of the small group of regulators and law-makers who have the structural power to change some of these practices and imbalances.

The absent presences within the general public sphere, and therefore in this article, are the perspectives of the children, parents and families who use, love, hate and/or fear these IoToys products. However, the recent emergence of 'unboxing' and 'let's play' YouTube videos centred around connected toys sees children now targeted across media platforms and co-opted as quasi-marketers, either through professionally based channels or by amateur child vloggers who 'mimic the production and branding strategies of the professional channels' (Nicoll & Nansen, 2017). This intricate transmedia relationship, where children's play (media mimicry) and content production intersect with the commercial world, needs further thought and analysis.

Acknowledgments

This research was supported by Dr Donell Holloway's ARC DECRA grant Digital Play: Social Network Sites and the Well-being of Young Children, ID: DE140101978, and by an ARC Discovery grant, Toddlers and Tablets: Exploring the Risks and Benefits 0–5s Face Online, DP150104734. This research is also partly supported by a European Cooperation in Science and Technology Grant, The Digital Literacy and Multimodal Practices of Young Children (DigiLitEY) ID: ISCH COST Action IS1410.

References

BBC (2017). German parents told to destroy Cayla dolls over hacking fears. *BBC News*, 17 February, http://www.bbc.com/news/world-europe-39002142.

Adhikari, R. (2015). Hello Barbie. Can we talk about your security issues? Technewsworld.com, 8 December, http://technewsworld.com/story/82842.html.

Barrett, B. (2016). ThingMaker is for kids, but you'll want this 3-D printer for yourself. *Wired*, 18 February.

Biber, D. (1995). *Dimensions of Register Variation*. Cambridge: Cambridge University Press.

Bogart, N. (2015). Security experts allege Hello Barbie can be hacked and used to spy on kids. *Global News*, 27 November, http://globalnews.ca/news/2366149/security-experts-allege-hello-barbie-can-be-hacked-and-used-to-spy-on-kids.

—— (2016). Hacked toy maker VTech changes terms to say it's not liable for data breaches. *Global News*, 10 February, http://globalnews.ca/news/2508781/hacked-toy-maker-vtech-changes-terms-to-say-its-not-liable-for-data-breaches.

BEUC (2016). EU & US consumer take action against flawed connected toys. BEUC the European Consumer Organisation, http://www.beuc.eu/press-media/news-events/eu-us-consumer-take-action-against-flawed-connected-toys.

Caldwell, T. (2011). Ethical hackers: Putting on the white hat. *Network Security*, 7, 10–13.

Chester, R. (2017). Millions of recorded messages between parents and children targeted in teddy bear toy hack. News.com.au, 28 February, https://perma.cc/7269-PC47.

Cohen, S. (2002). *Folk devils and moral panics: The creation of the mods and rockers (*3rd ed.). London: Routledge.

EPIC (2016). In the matter of Genesis Toys and Nuance Communications. Electronic Privacy Information Centre complaint to the US Federal Trade Commission, https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf.

eSafety (n.d.). eSafety Christmas gift guide. Office of the Children's eSafety Commissioner, https://esafety.gov.au/education-resources/iparent/resources/esafety-gift-guide.

European Commission (2017). Commission, data protection and consumer protection authorities look into issues with connected toys and apps. EU Media Release, http://europa.eu/rapid/press-release_MEX-17-741_en.htm.

Fairclough, N. (1992). *Discourse and Social Change*. Cambridge: Polity Press.

—— (1995). *Critical Discourse Analysis: The Critical Study of Language*. London: Longman.

Fram, S.M. (2013). The constant comparative analysis method outside of grounded theory. *The Qualitative Report*, 18, Article 1, http://www.nova.edu/ssss/QR/QR18/fram1.pdf.

Giddings, S. (2017). Pokémon Go as distributed imagination. Mobile Media & Communication 5(1), 59-62

Grimes, S. M. (2015). Playing by the market rules: Promotional priorities and commercialization in children's virtual worlds. Journal of Consumer Culture, 15(1), 110-134

The Guardian (2017). Germany bans children's 'smart' watches over surveillance concerns. *The Guardian*, 18 November, https://www.theguardian.com/technology/2017/nov/18/germany-bans-childrens-smart-watches-over-surveillance-concerns.

Hansen, F. & Christensen, L.B. (2005). Share of voice/share of market and long-term advertising effects. *International Journal of Advertising*, 24(3), 297–320.

Holloway, D. & Green, L. (2016). The Internet of Toys. *Communication Research and Practice*, 2(4), 506–19.

Hunt, T. (2017). Data from connected CloudPets teddy bears leaked and ransomed, exposing kid's [sic] voice messages. TroyHunt.com, 28 February, https://perma.cc/SZE5-QSFC.

Jayemanne, D. & Nansen, B. (2016). Parental mediation, YouTube's networked public, and the 'baby-iPad encounter': Mobilizing digital dexterity. *Jeunesse: Young People, Texts, Cultures*, 8(1), 133–53.

Keller and Heckman (2016). *US and EU Consumer Groups Ask Global Regulators to Investigate Two Connected Toys*. Washington: Keller & Heckman LLB, https://www.khlaw.com/9851.

Lankshear, C. & Knobel, M. (2011). *New Literacies: Everyday Practices and Classroom Learning* (3rd ed.). Maidenhead: Open University Press.

Livingstone, S. & Third, A. (2017). Children's and young people's rights in the digital age: An emerging agenda. *New Media & Society*, 19(5), 657–70.

Lupton, D. (2013). Infant embodiment and interembodiment: A review of sociocultural perspectives. *Childhood*, 20(1), 37–50.

Macnamara, J. (2005). Media content analysis: Its uses; benefits and best practice methodology. *Asia Pacific Public Relations Journal*, 6(1), 1–23.

Marsh, J., Hannon, P., Lewis, M. & Ritchie, L. (2017). Young children's initiation into family literacy practices in the digital age. *Journal of Early Childhood Research*, 15(1), 47–60.

Mascheroni, G. & Holloway, D. (eds) (2017). *The Internet of Toys: A Report on Media and Social Discourses Around Young Children and IoToys*. DigiLitEY, http://digilitey.eu/wp-content/uploads/2017/01/IoToys-June-2017-reduced.pdf.

Moini, C. (2017). Mandated ethical hacking: A repackaged solution. *Richmond Journal of Law and Technology Annual Survey*, 23, http://jolt.richmond.edu/volume23_annualsurvey_moini.

Mlot, S. (2016). Internet-connected toys provide joy (and surveillance). *Fox News*, 9 December, http://www.foxnews.com/tech/2016/12/09/internet-connected-toys-provide-joy-and-surveillance.html.

Mosco, V. (2009). *The Political Economy of Communication* (2nd ed.). London: Sage.

Newman, L.H. (2015). Internet-connected toys are getting hacked and it's as creepy as we feared it would be, Future Tense, 30 November, http://www.slate.com/blogs/future_tense/2015/11/30/researcher_matt_jakubowski_says_he_hacked_mattel_s_hello_barbie.html.

Nicoll, B. & Nansen, B. (2017). Toy unboxing videos and the mimetic production of play. Paper presented at the Digitising Early Childhood conference, Perth, http://www.digitisingearlychildhood.com/uploads/9/4/9/2/94929330/nicoll_toy_unboxing_videos.pdf.

PenTestPartners (n.d.). New, easier ways to make My Friend Cayla swear. Blog: Android, Penetration Testing and Security Services, https://www.pentestpartners.com/blog/new-easier-ways-to-make-my-friend-cayla-swear.

Roberts, J. (2016). Privacy groups claim these popular dolls spy on kids. *Fortune: Tech*, 8 December, http://fortune.com/2016/12/08/my-friend-cayla-doll.

SBS News (2015). VTech hack shows dangers of 'smart' toys: Expert. *SBS News*, 2 December, http://www.sbs.com.au/news/article/2015/12/02/toymaker-vtech-says-data-64-million-kids-hacked.

Singleton, M. (2017). Germany bans smartwatches for kids and asks parents to destroy them. *The Verge*, 19 November, https://www.theverge.com/circuitbreaker/2017/11/19/16671428/germany-bans-smartwatches-kids-parents-destruction.

Slettemeås, D. (2009). RFID: The 'next step' in consumer–product relations or Orwellian nightmare? Challenges for research and policy. *Journal of Consumer Policy*, 32(3), 219.

Swist, T., Collin, P., McCormack, J. & Third, A. (2015). *Social Media and the Wellbeing of Children and Young People: A Literature Review*. Perth: Commissioner for Children and Young People, http://www.uws.edu.au/__data/assets/pdf_file/0019/930502/Social_media_and_children_and_young_people.pdf.

Tait, A. (2016). Are smart toys spying on our children? *New Statesman*, 6 December, http://www.newstatesman.com/science-tech/privacy/2016/12/are-smart-toys-spying-children-0.

Thiesse, F. (2007). RFID, privacy and the perception of risk: A strategic framework. *The Journal of Strategic Information Systems*, 16(2), 214–32.

Timms, P. (2015). Hello Barbie: Wi-fi-enabled doll labelled a bedroom security risk. *ABC Online*, 28 November, http://www.abc.net.au/news/2015-11-27/wi-fi-enabled-hello-barbie-doll-raises-security-concerns/6981528.

Tyni, H., Kultima, A., Nummenmaa, T., Alha, K., Kankeinan, V. & Mäyrä, F. (2016). *Hybrid Playful Experiences: Playing Between Material and Digital. Hybridex Project: Final Report.* Helsinki: University of Tempere.

VTech (2016). FAQ about cyber attack on VTech Learning Lodge. *VTech*, https://www.vtech.com/en/press_release/2016/faq-about-cyber-attack-on-vtech-learning-lodge.

Wakefield, J. (2017). Germany bans children's smartwatches. *BBC News*, 17 November, http://www.bbc.com/news/technology-42030109.

Walker, H. (2017). Terrified German parents urged to destroy doll 'that can spy on children'. *Daily Express*, 18 February, http://www.express.co.uk/news/world/768924/My-Friend-Cayla-German-parents-childs-doll-destroy-hacking-internet-smart-technology.

Wallop, H. (2014). Meet Cayla, the first internet connected doll. *Daily Telegraph*, 5 November, http://www.telegraph.co.uk/finance/newsbysector/retailandconsumer/10881303/Meet-Cayla-the-first-Internet-connected-doll.html.

Walsh, M. (2017). My Friend Cayla doll banned in Germany over surveillance concerns. *ABC News*, 18 February, http://www.abc.net.au/news/2017-02-18/my-friend-cayla-doll-banned-germany-over-surveillance-concerns/8282508.

Wonder Toys (n.d.). Wonder Workshop [toy promo site], https://teachers.makewonder.com.