Surveillance capitalism and children’s data: the Internet of toys and things for children

Donell Holloway
Edith Cowan University, Australia

Abstract
This article discusses the positioning of children both as objects of economic activity as and subjects of market relations under surveillance capitalism. It looks briefly at the history of children’s engagement with the market economy from their engagement in the labour force during industrial revolution times; their disappearance from direct economic activity during the Romantic Movement; through to their emergence as both data sources and data consumers within a big data economy. It argues that this is the first time since children retreated from the paid labour force in the late 19th and early 20th centuries due to labour law reforms that their activities are of significant economic value, and that the emergence of Internet-connected toys and things for children will significantly amplify children’s position as data sources under surveillance capitalism.

Keywords
big data, children, datafication, dataveillance, datified child, Internet of toys, IoTT, surveillance capitalism

Introduction
Surveillance capitalism refers to new economic conditions in which online information (data) is converted into valuable commodities, and where the capture and production of these commodities (data) rely on mass surveillance over the Internet. In comparison to post-Fordist production practices, where the economy moved away from the office and factory, towards an economy progressively reliant on a ‘knowledge economy’, surveillance capitalism takes into account newer ‘big data’ practices which rely on the monetisation of people’s online data. These data are often extracted from the same population that will be eventually be its targets (Zuboff, 2014).

The Cambridge Analytica revelations, for example, have highlighted the extent to which Internet companies surveil the activities of digital citizens and how this can substantially shift the balance of power. Citizens’ data are captured, stored, monitored, analysed and on sold to commercial entities including ‘other online platforms, data brokers, intelligence agencies, and public administrations’...
Cambridge Analytic’s actions infringed upon Facebook’s own access regulations by carrying out data scraping, analytics and targeted on-selling under the pretence of academic research (Dwoskin and Romm, 2018). Their dealings also violated election interference regulations in the United Kingdom and United States. Despite the illegality of Cambridge Analytics actions, the bigger players and leading actors, Facebook and Google, are still legally amassing as much information as they can about specific users, their online friends and their offline friends (through shadow profiling) and making huge profits largely through facilitating micro-targeting by advertisers (Harris, 2018; Zuckerman, 2018). In this sense, Cambridge Analytica ‘is the little kids department when compared to what Facebook does’ (Kulcha, 2018: 22).

In the case of children, questions have long been raised about children’s data privacy in relation to children’s websites and apps (Grimes, 2008; Montgomery, 2002; Steeves, 2006). The advent of Internet-connected toys and children’s wearables, along with devices and apps not actually intended for children such as smart home assistants, provides significantly amplified opportunities for the appropriation of children’s data for commercial profit within a surveillance economy. Thus, concerns have been raised about how the commercial appropriation of children’s online information in the era of connected things further compromises the privacy and data security of children; often from children who are too young to consent to or understand the implications of this practice (Baraniuk, 2016; Harris, 2017; Holloway and Green, 2016). In addition to this, the consequences of accumulated data over a child’s lifetime – which will quickly outstrip the data accumulated on their parents – is of fundamental concern (Mascheroni and Holloway, 2018).

Using a Political Economy framework, this article investigates the positioning of children both as objects of economic activity (as data sources) and subjects of market relations (as digital consumers) under surveillance capitalism (Andrejevic, 2014; Zuboff, 2015). It traces the history of children’s engagement with the market economy, through to their emergence as both data sources and data consumers within a big data economy. The article highlights how the emergence of connected things for children complicates and amplifies the significance of children’s data for commercial entities within a surveillance economy. First, and despite having already been purchased and owned by consumers, the presence of embedded and connected software in children’s toys and wearables means that the customer is subject to long-term contractual obligations. These terms and conditions enable data exchange between the child and the platform; the child and parent; and the child and other data sharing recipients. Furthermore, the assortment of sensors embedded in Internet of toys and things (IoTTs) for children provides new datasets that are already being captured and datafied (Lupton and Williamson, 2017). These new data sources include children’s voices, movements, locations, images, breathing and heartbeat patterns. Consequently, the connection of children to the Internet through their bodies, play, learning and social interactions further heightens children’s re-entry into the economy both as economic objects and subjects.

**Surveillance capitalism in the lives of children**

As a new version of capitalism, surveillance capitalism monetizes data obtained through surveillance (Zuboff, 2015). The term surveillance capitalism was coined by academic Shoshana Zuboff. She suggests that surveillance capitalism depends on ‘a global architecture of computer mediation … which produces a distributed and mostly uncontested new expression of power that that I christen: “Big Other”’ (p. 75). The biggest ‘Big Other’ actors at this stage are Google, Amazon, Facebook and Apple who in combination collect and control unparalleled quantities of data about their users activities which they turn ‘into products and services that have fuelled stunning commercial growth’ (Moore, 2016: ii).
This corporate practice was first consolidated at Google. Through the use of ‘illegible mechanisms of extraction, commodification, and control’ (Zuboff, 2015: 75), new markets are created for the use of personal data. This ‘Big Other’ concentration of power over data ownership, security and privacy puts at risk personal and collective freedoms; Cambridge Analytics data misuse being the prime example of the day. In addition to this, our expanding sensor-based society (IoTTs) is now driving the intensification of connection and monitoring online beyond the spaces of online social and consumer life to an ever expanding list of activities such as self-tracking, smart homing, health analytics, automated travel, school analytics and more.

Babies and children are clearly embedded actors within surveillance capitalism. Many unborn children now have an online presence. Expectant parents often announce their pregnancy by posting an ultrasound image of their foetus on Facebook, Instagram and Pinterest (Leaver, 2017). This sharing practice is now being expanded and elaborated on with new rituals and postings, such as videos of ultrasound clinic visits, gender reveal parties, infertility journey videos and memorials for stillborn children. These postings usually include ultrasound images and other more detailed information about the unborn child (Mascheroni and Holloway, in press).

Once born, babies’ online presence continues with parent postings which often share the name, gender, birth weight and birth date of the newborns. Data are also captured via increasingly popular baby wearables, monitoring devices that are fastened close to babies’ bodies that collect information via Bluetooth and wifi technologies about babies’ health, location or identity (Mascheroni and Holloway, 2018). Further data collection, analysis and sharing occur across a child’s different life stages. Toddlers are choosing and viewing videos on YouTube and once they enter the education system, the datafication of many aspects of children’s lives continues and expands. The tracking of their learning activities and achievements, classroom behaviour, sport activities and health parameters at school adds further data which now supplements and far outweighs data collected from parental postings (Mascheroni and Holloway, in press).

Two recent events highlight how surveillance capitalism is clearly taking place in the lives of children regardless of existing privacy regulations and rules such as the US Children’s Online Privacy Protection Act (COPPA), the EU General Data Protection Regulation and the future ePrivacy Regulation. First, researchers from The University of California have recently released results on their analysis of the privacy practices within 5855 children’s Android apps. They found that over half the apps analysed potentially violated COPPA and suggest that ‘it is not clear that industry self-regulation has resulted in higher privacy standards; some of our data suggest the opposite. Thus, industry self-regulation appears to be ineffective’ (Reyes et al., 2018: 77). Second, on-selling or sharing of children’s data is also occurring at an intensive rate. Recent figures released by AdTech, a London-based digital marketing firm, shows that by the time a child turns 3 or 4, five million data points have been collected by ‘adult Adtech delivering ads into kids and family digital content’ (Harris, 2017). This rises to 72 million data points before a child reaches the age of 13. AdTech’s use of data collection technology, which was initially built to capture adult users’ data, now collects information about a child’s location, apps used, websites visited and device identifiers, as well as more specific personalised data (Harris, 2017).

This not only breaches children’s privacy regulations but creates a new data-rich environment that is changing power structures in a data economy which now operates without any meaningful procedures for individual consent (Zuboff, 2015). This is particularly significant in the lives of children as they are often too young to understand or consent (or who may not even be born, if their parents post ultrasound scans). The future ramifications in terms of children’s sense of self and healthy development, and their future ability to find, own, reclaim, contest or delete information about themselves is uncertain.
Children’s engagement in the market economy: then and now

Before the 18th century, children usually laboured alongside their parents. In pre-industrial societies, children usually worked in childcare, hunting or gathering, farming and cottage crafts as soon as they were competent. While children from poorer families were expected to contribute to the economic survival of their family unit, social class was responsible for some variation in the lives of children, with upper-class children seldom put to work (Fyfe, 2005).

Child as labourer

During the 19th century, child labour was seen as an economic opportunity rather than an ethical problem, especially for poor families. Families moved to growing industrial cities so that they could make a better living. However, extremely low wages led families to supplement their household income by sending their children off to work as well. With growing production rates, the industrial revolution also provided the chance for children to find work that, before then, was hard to find. Indeed, historians suggest that by the 1830s, the more industrialised a nation was, the more child labour opportunities there were (Fyfe, 2005).

The end of the 19th century saw the end of widespread child labour. This decline occurred in stages with 5- to 9-year-olds being the first to leave the workforce around the 1850s, then 10- to 14-year-olds in the 1870s. However, children over 14 years of age remained in the workforce in high numbers into the first few decades of the 20th century. There are a variety of reasons for the decline of child labour in the United States and Europe. First, as income levels increased, especially for the male household head, families could afford to choose to ‘invest in their children by sending them to school’ (Fyfe, 2005: 4). In addition, as technology became more sophisticated and machines could undertake more tasks, the demand for child labourers declined. Ideological changes of the Romantic Movement, which demarcated childhood as a stage of life where child should be free from the commitment of work and live a pleasurable and dependent lifestyle, put pressure on the state to provide all children with the right to be free from work. These ideological changes, along with frightful working conditions children laboured under, then saw changes to the law with a series of Acts which progressively regulated children out of the workforce. These included the 1833 Factory Act in Britain and the 1864 Factories Act (extension) Act which reduced the number of child labourers in potteries, the 1860 Mines Regulation and Inspection Act which banned boys under 12 from working underground, and child labour regulations in Russia (1839), France (1874) and the United States (1993). In addition to this, compulsory education was introduced in the late 1800s. For example, after the 1870 Education Act, it became compulsory for children age between 5 and 10 to attend school in Britain and a series of reforms in the 1880s required children attend school in France (Fyfe, 2005). These reforms saw children effectively retreat from the paid labour force into the domestic realm of home and school.

Child as consumer

The emergence of a product aimed at children can be traced back to the 16th century where books, toys and clothes were made for the children of wealthy bourgeoisie and nobility (Luke, 1989) although larger scale production began in the 18th century. This move to recognise children as nascent commercial targets came about because of three main reasons. The earlier conceptual shift in the late 1800s towards the Romantic notion that children personify a state of innocence, purity and the goodness of nature, but who could be corrupted by the world outside, left children (especially middle- and upper-class children) separated from adults and sequestered in the domestic
Holloway

realm. This distinctiveness and separateness was then used in the commercial world as a way to ‘connect the child to the market’ (Cook, 2004: 23). In other words, new market meanings and categories constructed the child as essentially separate and different from adults to create a distinct market niche. Distinctive children’s products emerged with separate children’s departments appearing in larger department stores and new advertising aimed directly at children (Ellis, 2011).

Children’s consumption is also associated with developments in the media and cultural industries. While media is itself a product for children to consume, it also played a major role in shaping children’s consumer culture (Buckingham, 2011). Children’s media texts often connected to other commodities of interest to children. Illustrated stories and comic strips which introduced characters whose images appeared in dolls, games and toys were available from the 1890s. By 1937, Disney had mastered the art of tie-in marketing by selling Snow White and the Seven Dwarfs merchandise even before the movie was released. Over time, childhood became linked with a vast interconnected industry built on licenced characters that encompassed movies, TV shows, video games, toys and clothing. Moviemakers often joined forces with toy and fast food companies to offer novelty toys in fast food meals. Video games, in the mid-1970s, first directed towards teens and young adults, were marketed to children in the late 1970s with Atari, and by Nintendo and others by the late 1980s. In addition, media-generated marketing to children created consumption practices, where children were encouraged to accumulate whole ‘sets’ of dolls, toys, books and videos. This marketing became ever more sophisticated with the Star Wars trilogy (1977–1983). In addition to this, cartoon series based on existing toy and doll lines proliferated from the 1980s onwards (Ellis, 2011).

Contemporary marketing to children is integrated with newer digital technologies.

Over the past twenty years, digitization has led to the emergence of a whole range of new technologies of production, distribution and consumption. Previously distinct media forms and commodities have begun to converge, as television programmes are linked to websites, films and computer games – and, of course, to merchandising and advertising. (Buckingham, 2011: 84)

A diverse range of integrated marketing techniques is used to engage and capture children’s attention. Product and brand placements occur within online virtual worlds and gaming sites. Advergaming, the use of video game platforms to promote products to children, is also used, as well as the use of data mining in order to provide more personalised (wants and needs) advertising to children (Buckingham, 2011). Buckingham (2011) described data mining as ‘the gathering of data about consumers based on their responses to online requests, or (more covertly) through the use of cookies that track their movements online’ (2011: 99). These data mining activities have since evolved and expanded over a short period to produce ‘treasured resources that can ostensibly be mined, enriched, and repurposed into precious products’ (van Dijck, 2014: 199) themselves.

Child as data source

These days, children have been again inducted into the market economy as economic objects. This time, however, it is the data they supply rather than their direct physical labour that have economic value under surveillance capitalism. These data include information about children’s interactions and content creation in virtual worlds and social networks, self-tracking of children via baby wearables, watches, fit-bits, connected toys and smartphones. For example, young YouTube viewers provide YouTube viewer data on highly viewed videos within a 2- to 5-year-old age range which is then provided to advertisers to create company profit. Pokemon Go, as a location-based game, collects the names and locations of its users. However, it also accesses the contents of children’s
USB storage, their accounts, photographs, network connections and phone activities, and can even activate their device, when it is in standby mode. Niantic, Pokemon Go’s developer, also reserves the right to share all the data it collects with third parties, such as digital marketing firms and advertisers, to enable it to bring in extra revenue (Rottenberg, 2016).

Under surveillance capitalism, and thanks to much improved technical capacities such as improved storage and AI (artificial intelligence) analytics and an increasing number of data sources, commercial entities have increasing access to larger volumes of data for the marketing and sale of products and services (including the on-selling of datasets). Thus, children’s movements, bodies, play activities, communications and social and cognitive development are now digitisable and commodifiable. This data surveillance also tends to normalise a surveillance culture by making what was once an uncommon practice (digital surveillance) so common that it seems unremarkable. Nonetheless, the long-term consequences on children’s self-development are hard to predict (Mascheroni and Holloway, 2018).

While the collection and use of children’s data raise issues regarding children’s privacy, concerns have also been raised about the loss of control of personal data, as well as ‘the potential for direct or inadvertent discrimination and profiling, scope creep and technological dependency – resulting in restrictions on access to vital services’ (Berman and Albright, 2017: 20). Children’s data can be subject to collection and analytical procedures that skew results and discriminate against individual children or groups of children. This occurs when algorithms are based on inaccurate assumptions about a vulnerable group of children when using data such as health profiles or geolocation. It also occurs when there is underrepresentation or overrepresentation of a vulnerable or marginalised cohort of children leading to incorrect inferences and decisions being made. Furthermore, these skewed results and subsequent discrimination also happens as a result of an overreliance on a specific data source. In this case, more detailed and verifiable methods or multiple methods which enables triangulation of results are disregarded (Barocas, 2014). Another driver of this discrimination is when datasets are moved out of the context in which they were collected (by on-sellers and data brokers), thus becoming more unreliable (Nissenbaum, 2009). School behavioural data, for instance, data found in classroom behaviour modelling apps such as ClassDojo, may be taken out of a local, class and age-based context and used to assess and categorise an individual’s behaviour beyond the context of the child’s age and their specific classroom.

While the collection of children’s data can produce skewed and discriminatory data, it can also result in both indirect and direct benefits for children. In the field of education, data collection and analytics provide information that can personalise children’s learning and provide supportive interventions to enhance educational opportunity. Health care provision (both preventive and responsive care) is also enhanced through big data analysis. Aggregated and disaggregated data can be used to identify groups or locales in need of certain prevention or mitigation services – such as the tracking of communicable diseases and the provision of vaccination services. The identification of young children in crisis mapping operations facilitates the provision of food and shelter to these children who are particularly susceptible to malnourishment and death (Moestue and Muggah, 2014). The detection of crimes such as child abuse is enhanced through the use of data analysis. Abusers and distributors of child abuse materials are currently being tagged while online or in cloud-based storage – and more readily identified and located by crime enforcement bodies (Berman and Albright, 2017).

The case of connected toys

Highly publicised breaches involving connected toys highlight the economic value of children’s data under surveillance capitalism. These breaches include the hacking of Mattel’s Wi-Fi Hello
Barbie™ (Nov, 2015), VTech’s Learning Lodge™ (Nov, 2015) and CloudPets™. Other hacks or breaches have been carried out by consumer groups and ‘white hat’ hackers who point out the lack of data protection built into connected toys and their support infrastructure. Research carried out by the Norwegian Consumer Council (2017) related to Genesis’ toys, My Friend Cayla™ and iQue Intellegeny Robot™ (Bureau Européen des Unions de Consommateurs, 2016) and children’s smart watches point towards these vulnerabilities. In addition, the German government has named My Friend Cayla™ doll (a toy similar to Hello Barbie™) as an ‘illegal espionage apparatus’ because ‘under German law it is illegal to manufacture, sell or possess surveillance devices disguised as another object’ (Walker, 2017). Later that year, the same government banned the use of children’s smart watches because ‘Via an app, parents can use such children’s watches to listen unnoticed to the child’s environment and they are to be regarded as an unauthorised transmitting system’ (Wakefield, 2017).

When IoToys data breaches are made public, the size and significance of the data held by IoToys manufacturers and their service providers are also made clear. In the case of the 2015 VTech breach, ‘about 2.2 million parents had registered and created accounts with Learning Lodge for nearly 3 million children’ (Federal Trade Commission, 2018). A more recent data breach, on CloudPets™ database left over 820,000 user accounts open to theft. The user profiles included profile photos, children’s names, as well as the month and day of their birth. The profiles also contained the child’s relationship to adults who have been authorised to share messages with the child, such as parents, grandparents and aunts (Hunt, 2017). At this stage, it seems that some toy manufacturers lack the technical expertise or are hesitant to employ or contract out this expertise in order to sufficiently protect children’s data – and little transparency or independent oversight takes place at this stage regarding children’s online data.

CloudPets™ data breach

Children’s voices and data were leaked during a data breach involving CloudPets™ database in 2017. CloudPets™ are Internet-connected soft toys made by Spiral Toys, based in California. These toys allow parents and their children to send voice messages to each other through the toy itself. The toys are embedded with Bluetooth Low Energy (BLE) technology that connects to parents’ smartphones so that up to six family members can send voice messages to the toy, and the child can send voice messages back. The app enabled toys can also play lullabies and narrate children’s stories via the toy’s speakers. Family members use the CloudPets™ app to send messages to their children and children use the toy itself to receive and send messages. Children squeeze the toy’s left paw to receive messages and the right paw to record messages to be sent via cloud storage to family members (Jackobson, 2015).

Security expert and creator of Have I Been Pwned? (a data breach search website that allows the general public to see if their personal information has been compromised) found that the CloudPets™ database had been breached in February 2017. He noted that children’s data were stored in a highly insecure database, a ‘MongoDB that was in a publicly facing network segment without any authentication required and had been indexed by Shodan (a popular search engine for finding connected things)’ (Hunt, 2017). At the time, the database held over 2,182,337 voice recordings from both children and adults. Hunt and others followed the database comings and goings over a 6-week period noting that ‘CloudPets data was accessed many times by unauthorised parties before being deleted and then on multiple occasions, held for ransom’ (Hunt, 2017).

Over this period, many attempts were made to notify Spiral Toys by email and telephone. Messages were also left on the company’s Facebook and Twitter accounts. These messages went
unanswered. Over this same period, parents were not informed of the breach by Spiral Toys, a requirement of the Californian government where the company is located (Hunt, 2017).

Hunt was notified of the breach by an acquaintance involved in data breach trading circles. These trading circles redistribute stolen databases extensively for either financial gain or as a hobby. The breached databases ‘often spread well beyond the party that originally obtained it and the ease with which huge volumes of digital information can be replicated across the globe means that once it’s exposed, it spreads rapidly’ (House Committee on Energy and Commerce, 2017: 2). In his testimony to the US House Committee on Energy and Commerce (2017) ‘Identity Verification in a Post-Breach World’ inquiry, Hunt also noted that

The rapid emergence of cheap, easily accessible cloud services has accelerated the growth of other online services collecting data. Further to that, the rapidly emerging ‘Internet of Things’ is enabling us to digitise all new classes of information thus exposing them to the risk of a data breach. (p. 2)

To date, Spiral Toys and other toy manufacturers have been allowed to self-regulate with regard to data privacy and safety. The CloudPets™ event, nonetheless, indicates that the rapid uptake of cheaper cloud-based database platforms is part of the problem in that these databases are often unsecured and easily hacked. Some toy companies, for instance, Cognitoys, are taking their responsibilities seriously and incorporate best practice in their toy design and infrastructure security (Knowles et al., 2018). Others, such as Spiral Toys, generally lack the skill set and technical infrastructure required to venture unsupported into the IoToys space. Given the current susceptibility of IoToys to hacking at a local (Bluetooth) level as well as database level, it is obvious that this self-regulatory environment is not working.

Conclusion

Contemporary childhood has (and is) undergoing a profound transformation, where information about children’s bodies, play and social interaction is migrating to the digital realm. Industry has taken note of these changes, creating many opportunities for children to be tracked, play and socialise online including new, screen-less platforms such as wearables, virtual assistants and connected toys. At the same time as industry is creating opportunities for children’s cultural participation online, they are, however, gathering vast amounts of user/child information, either surreptitiously or with the consent of children or parents – who recognise that opting out of data collection and sharing practices may diminish the user experience. In addition, a digital black market is emerging where children’s data are traded within data breach trading circles or held for a bitcoin ransom.

This is the first time since children retreated from the paid labour force in the late 19th and early 20th centuries that their activities are of any significant economic value. Under surveillance capitalism, children have been positioned as data sources and at the same time subjects of market relations. The use of wearables, virtual assistants and connected toys equipped with a growing number of sensors such as audio, visual, haptic, location, temperature and moisture sensors (think smart nappies) increases the number of transmission points and data points and lifts data collection possibilities to a whole new level.

As new technologies are designed to capture and respond to children’s everyday experiences more and more seamlessly, their bodies, activities and social experiences are being tracked and datified. While there is a need to educate children and their parents about digital data collection and ownership and how this may have an effect on them into the future, of greater importance (in terms of children who are often too young to consent or understand the full possible consequences of
their consent) is the need for consolidated work towards a code of conduct and further regulation with regard to the ownership of children’s data from production through to sale.

**Declaration of conflicting interests**

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

**Funding**

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This article is part of an Australian Research Council project *The Internet of Toys: Benefits and risks of connected toys for children* (DP 1801039220).

**ORCID iD**

Donell Holloway https://orcid.org/0000-0003-2202-5551

**References**

Andrejevic M (2014) Surveillance in the big data era. In: Pimple KD (ed) Emerging Pervasive Information and Communication Technologies (PICT). New York: Springer, pp. 55–69

Baraniuk C (2016) Call for Privacy Probes Over Cayla Doll and I-Que Toys. London: British Broadcasting Corporation.

Barocas S (2014) Data mining and the discourse on discrimination. In: *Data ethics workshop, conference on knowledge discovery and data mining*, New York, 24–27 August.

Berman G and Albright K (2017) Children and the Data Cycle: Rights and Ethics in a Big Data World [Working Paper]. Florence: UNICEF Innocenti Research Centre.

Buckingham D (2011) The Material Child: Growing Up in Consumer Culture. Cambridge: Polity Press.

Bureau Européen des Unions de Consommateurs (2016) EU & US consumer take action against flawed connected toys. BEUC NEWS. Brussels: The European Consumer Organisation.

Cook DT (2004) *The Commodification of Childhood: The Children’s Clothing Industry and the Rise of the Child Consumer*. Durham, NC: Duke University Press.

Dwoskin E and Romm T. (Mar 19 2018) Facebook’s rules for accessing user data lured more than just Cambridge Analytica. *Washington Post*. Washington DC. Available at: https://www.washingtonpost.com/business/economy/facebook-rules-for-accessing-user-data-lured-more-than-just-cambridge-analytica/2018/03/19/31f6979e-658e-43d6-a71f-afdd8bf1308b_story.html?utm_term=.73d5023e0ddf.

Ellis L (2011) Towards a Contemporary Sociology of Children and Consumption (Applied social sciences). Durham: Durham University.

Federal Trade Commission (2018) Electronic Toy Maker VTech Settles FTC ‘legations that it Violated Children’s Privacy Law and the FTC Act. ~ Washington, DC: Federal Trade Commission.

Fyfe A (2005) Compulsory Education and Child Labour: Historical Lessons, Contemporary Challenges and Future Directions (Working Draft). International Labour Organization. Available at: http://www.ilo.org/ipeclinfo/product/viewProduct.do (accessed 12 August 2018)

Grimes SM (2008) Kids’ ad play: regulating children’s advergames in the converging media context. *International Journal of Communication, Law and Policy* 8: 161–369.

Harris M (2017) 72M data points collected on children in spite of COPPA. *App Developer Magazine*. Available at: https://appdevelopermagazine.com/72m-data-points-collected-on-children-in-spite-of-coppa/

Harris M (2018) The Cambridge Analytica Saga is a Scandal of Facebook’s Own Making. London: Guardian Media Group. Available at: https://www.theguardian.com/commentisfree/2018/mar/21/cambridge-analytica-facebook-data-users-profit

Hintz A, Dencik L and Wahl-Jorgensen K (2017) Digital citizenship and surveillance digital citizenship and surveillance society – Introduction. *International Journal of Communication* 11: 731–739.

Holloway D and Green L (2016) The Internet of toys. *Communication Research and Practice* 2: 506–519.
House Committee on Energy and Commerce (2017) *Identity Verification in a Post-Breach World* (USA Government, Testimony of troy hunt). Washington, DC: House Committee on Energy and Commerce.

Hunt T (2017) Data from connected CloudPets teddy bears leaked and ransomed, exposing kid’s voice messages. *Troy Hunt*. Available at: https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/

Jackobson J. (2015) *Cloudpets™*: The perfect companion when a parent is away. I can teach my child. Andover, Kansas. Available at: https://www.icanteachmychild.com/cloudpets-the-perfect-companion-when-parent-is-away/

Knowles B, Finney J, Beck S, et al. (2018) What children’s imagined uses of the BBC micro:bit tells us about designing for their IoT privacy, security and safety. In: *Living in the internet of things: cybersecurity of the IoT*, London, 28–29 March.

Kulcha H (2018) How do you like that Facebook? *Weekend Australian Magazine* Sydney: News Corp, pp. 21–23. 21 April.

Leaver T (2017) Born digital? Presence, privacy, and intimate surveillance. In: Hartley J and Qu W (eds) *Re-Orientation: Translingual Transcultural Transmedia: Studies in Narrative, Language, Identity, and Knowledge*. Shanghai, China: Fudan University Press, pp. 149–160.

Luke C (1989) *Pedagogy, Printing and Protestantism: The Discourse on Childhood*. Albany, NY: SUNY Press.

Lupton D and Williamson B (2017) The datafied child: the dataveillance of children and implications for their rights. *New Media & Society* 19: 780–794.

Mascheroni G and Holloway D (in press) The quantified child: discourses and practices of dataveillance in different life stages. In: Erstad O (ed.) *Routledge Handbook of Digital Literacies in Early Childhood*. Abingdon: Routledge.

Moestue H and Muggah R (2014) *Digitally Enhanced Child Protection: How New Technology Can Prevent Violence Against Children in the Global South*. Rio De Janeiro, Brazil: Igarape Institute.

Montgomery K (2002) Digital kids: The new on-line children’s consumer culture’. In: Carlsson U and von Feilitzen C (eds) Children, young people and media globalization. Gothenburg, Sweden: Nordic Information Centre for Media and Communication Research, 189–208.

Moore M (2016) *Tech Giants and Civic Power*. London: Centre for the Study of Media, Communication and Power, King’s College London.

Nissenbaum H (2009) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

Norwegian Consumer Council (2017) *WatchOut: Analysis of Smartwatches for Children*. Oslo: Norwegian Consumer Council.

Reyes I, Wijesekera P, Reardon J, et al. (2018) ‘Won’t somebody think of the children?’ Examining COPPA compliance at scale. In: *The 18th privacy enhancing technologies symposium*, Barcelona, 24-27 July.

Rottenberg J (2016) *Oliver Stone Calls ‘Pokemon Go’ ‘Surveillance Capitalism’*. Los Angeles, CA: Ross Levinsohn.

Steeves V (2006) It’s not child’s play: the online invasion of children’s privacy. *University of Ottawa Law and Technology Journal* 3: 169–188.

van Dijck J (2014) Datafication, dataism and dataveillance: big data between scientific paradigm and ideology. *Surveillance and Society* 12: 197–208.

Wakefield J (2017) *Germany Bans Children’s Smartwatches*. London: British Broadcasting Corporation.

Walker H (2017) *Terrified German Parents Urged to Destroy Doll That Can Spy on Children*. London: Northern and Shell Media.

Zuboff S (2015) Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology* 30: 75–89.

Zuboff S. (2014) The new weapons of mass detection. Frankfurter Allgemeine Feuilleton. Frankfurt: Fazit Foundation.

Zuckerman E (2018) *This Is So Much Bigger Than Facebook: Data Misuse Is a Feature, Not a Bug – and It’s Plauguing Our Entire Culture*. Boston, MA: Hayley Romer.