The datafied child: The dataveillance of children and implications for their rights

Deborah Lupton

News & Media Research Centre, University of Canberra, Australia

Ben Williamson

Faculty of Social Sciences, University of Stirling, UK

Pre-publication version of a paper published as:

Lupton, D. & Williamson, B. 2017. The datafied child: The dataveillance of children and implications for their rights. *New Media & Society*: http://journals.sagepub.com/doi/full/10.1177/1461444816686328

Abstract

Children are becoming the objects of a multitude of monitoring devices that generate detailed data about them, and critical data researchers and privacy advocates are only just beginning to direct attention to these practices. In this article we provide an overview and critique of these varied forms of datafication and dataveillance of children, from *in utero* through to the school years. Our approach is informed by recent calls for research on children's rights in the digital age that examines the conditions that give rise to children's needs and guide provision of resources necessary for development to their full potential; the array of specific harms they may encounter; and the significance of and particular opportunities to participate in matters that affect their wellbeing and enable them to play an active part in society. There remains little evidence that specific instruments to safeguard children's rights in relation to dataveillance have been developed or implemented, and further attention needs to be paid to these issues.

Keywords

digital data, children, rights, dataveillance, datafication, parents, education

Introduction

A host of scholarly publications since the advent of personal computing in the 1980s has directed attention to the ways in which children use digital technologies. However, little research thus far has sought to examine how children are the objects of a proliferating range of digitized surveillance practices that record details of their lives.

Children may engage in these practices themselves, but many other actors do so on their behalf, including not only their parents and other caregivers and family members, friends, teachers and healthcare providers, but also commercial entities seeking to capitalize on and profit from children's personal information. As a result, children have become increasingly datafied via such technologies as mobile media, wearable devices, social media platforms and educational software. The data generated by these technologies are often used for dataveillance, or the monitoring and evaluation of children by themselves or others that may include recording and assessing details of their appearance, growth, development, health, social relationships, moods, behaviour, educational achievements and other features.

While critics have begun to draw attention to the ways in which continual personal digital data generation is beginning to influence people's life chances and opportunities and to concerns about data privacy and security, few analyses have identified the implications for children. The dataveillance of children raises many important questions about children's rights. Livingstone (2016) has recently detailed how a concern for children's digital rights has begun to intersect with existing children's rights instruments such as the United Nations Convention on the Rights of the Child (UN CRC) (1989). Acknowledging that the UN CRC and World Wide Web both celebrated their 25th anniversaries in 2014, Livingstone argues that:

> Children's lives in the digital age raise new questions about the so-called 3P's of the CRC – rights to provision, protection and participation – in the changing media and communication environment.… As children's daily lives become ever more heavily mediated, and as the media themselves simultaneously converge and diversify, researchers along with policy-makers and the public are now debating whether "the digital age" is enhancing or undermining children's rights, with current controversies centring on children's right to privacy online as offline, to information and freedom of expression, and to protection from sexual and aggressive threats variously mediated and amplified by the internet. (Livingstone 2016: 5)

Our focus in this article is on privacy issues in relation to the digital data that are now generated incessantly about children as they participate online. First, we provide an overview of these varied forms of datafication and dataveillance of children in the countries of the Global North by presenting theoretical perspectives on the broader implications. This section is followed by descriptions of the types of practices and technologies that are employed, from before birth and through the school years. We then reflect on issues concerning the risks of dataveillance, such as the exploitation of digital data about children, their rights about the ways in which others collect and use data about them and data privacy and security. In the final part we develop the argument that while children's rights instruments such as the UN CRC have emphasized children's

'voice' and participation, datafication and dataveillance displace concerns for eliciting voice with a focus on 'objective' data that contains 'actionable insights' for future intervention in children's lives.

Modes of dataveillance and digital data assemblages

Analysing the datafication and dataveillance of children requires insights from perspectives on contemporary modes of surveillance as they operate via new digital technologies. In this age of ubiquitous computing, high levels of social media use and sensor-embedded physical environments (including public places fitted out with CCTV cameras, traffic flow monitors and drones), digital data about people's behaviours and bodies are ceaselessly generated, on their own behalf and by others. The term 'dataveillance' refers to collecting information using forms of data (Raley, 2013: 15; van Dijck, 2014). Dataveillance now frequently operates with the use of digital technologies and takes place at varying degrees of people's knowledge and consent. Individuals may voluntarily choose to engage in self-surveillance, for example, by using self-tracking devices and software (Albrechtslund and Lauritsen, 2013; Lupton, 2016). Another form of watching, that of 'intimate surveillance', describes the monitoring of other people that takes place as part of close personal relationships (such as those between family members and couples) (Albrechtslund and Lauritsen, 2013; Levy, 2015). People may invite others to watch them by participating in social media interactions and uploading personal details and images to sites such as Facebook, Twitter, YouTube, LinkedIn, Tumblr or Instagram. This type of consensual and mutual watching has been dubbed 'social surveillance' (Marwick, 2012) or 'participatory surveillance' (Albrechtslund and Lauritsen, 2013). These modes of dataveillance are part of the emergent phenomenon of conducting social and intimate relationships via the collection and perusal of data about each other.

Less consensual forms of dataveillance also take place. Some of these forms, as in the use of CCTV cameras, ascribe more closely to Foucauldian panoptic modes of surveillance, in which small numbers of people in positions of power observe large masses of citizens. While they may not have agreed to this surveillance, citizens know that they may be watched and modify their behaviour accordingly (Elmer, 2003). Digitized strategies of covert surveillance remain common, including not only the hidden sensors embedded into physical public spaces, but also internet companies' continual monitoring of online interactions for commercial purposes, and, as revealed by Edward Snowden, the dataveillance of citizens by national security agencies. Some critics have argued for an understanding of 'post-panoptic' forms of surveillance using digital technologies, whereby people are surveilled through partial or 'oligoptic' vantage points (Gane, 2012). Oligoptic surveillance is a particular feature of the combination and alignment of different datasets collected about people as part of their use of digital

technologies. These practices provide tiny details from a heterogeneous variety of sources to construct a novel data profile.

All of these forms of dataveillance contribute to what Lyon and Bauman (2013) refer to as 'liquid surveillance', or the dispersed and mobile watching of ourselves and each other facilitated by digital technologies that generates continuous flows of data about individuals. Once collected, these personal data tend to become part of the digital data economy, available for use by a variety of actors and agencies in ways that are often unknown to the people about whom this information relates (Kitchin, 2014; Lupton, 2015b). Most of the personal data generated are collected and stored on proprietary platforms that have a commercial motive to exploit these data. New power relations have formed around the uses of and access to people's personal data, with the internet empires such as Google, Facebook and Apple and other major corporations that collect and archive these data having far greater access to and the opportunity to profit from these data than citizens (Andrejevic, 2014; van Dijck, 2014).

The consequence of these techniques of dataveillance is that people are configured as 'digital data assemblages'. By using this term, we draw attention to how human actors and non-human objects interact to shape each other in a mutually constitutive relationship (or 'assemblage'). In the specific dataveillance context, Haggerty and Ericson (2000) refer to 'surveillant assemblages' as the aggregation of data sources that combine to produce a digital doppelganger of the individual, and represent human subjects as digital archives. Data assemblages are lively, constantly changing as new forms of information are produced and combined with other datasets. The transformation of people into data can encourage them to see themselves as data assemblages, or allow other external agencies to use the numbers to influence or act on individuals. As we demonstrate below, children are now often the subject of many of these dataveillance modes. Via dataveillance, they are rendered into data assemblages in ways that pose significant challenges for reconsidering their rights.

Dataveillance technologies directed at children

It is important to emphasize the novel features of new digital media technologies and their capacity for generating personal information about children. Children have been subjected to close monitoring as part of the government of childhood for centuries in an attempt to promote their health, development and educational progress, and to ensure that they become productive citizens (Bellman and Vijeratnam, 2012; Jenks, 2005). While developing *in utero* and from seconds after birth, children are positioned within intense networks of surveillance on the part of parents, healthcare workers and teachers. The new digital media and the emergence of the global knowledge economy that has valorized personal information for commercial, research, managerial and governmental purposes have brought with them unprecedented capacities for such monitoring of

children. Contemporary digital data technologies offer affordances that allow for continual and real-time data generation, archiving and tagging for ready retrieval of massive quantities of personal details about them.

Intimate surveillance has become a popular practice among parents in response to their infants and young children: a way of announcing a pregnancy to friends and family, sharing details of foetuses and children, and conducting monitoring of their unborn and children as part of parental care. The processes of dataficiation and dataveillance of children can begin from early gestation. The sharing on social media sites such as Facebook, Twitter, Instagram and YouTube of the first foetal ultrasound image is one of the ways in which parents now publicly announce the new pregnancy (Leaver, 2016; Lupton, 2013). More than 1,000 apps related to pregnancy are now available on the market, many of which provide opportunities for pregnant women to monitor the growth, development, movements and even heart rate of their foetuses (Lupton and Thomas, 2015; Thomas and Lupton, 2015). Some parents choose to share their photos and videos of the moment of birth on public sites such as Instagram and YouTube for any internet user to view (Leaver, 2016; Longhurst, 2009).

Once the infant is born, apps are available for parents to monitor such aspects as their infant's sleeping and feeding patterns, medication regime, development, growth and health. Parents may now purchase wearable devices, changing mats, baby scales, clothing, dummies, feeding bottles and toys embedded with sensors. These devices can record their children's biometric data such as heart and breathing rate, body position when sleeping, dietary intake, oxygen levels and skin temperature, all sent to the parents' smartphone apps in real time. One such device, the Sproutling ankle band, takes 1,000 measurements of the infant wearing it per minute. Smartphones turn into baby monitors with the use of apps such as 'Baby Monitor', which records the sound levels of the infant. Parents typically take a multitude of digital photographs and videos of their children from birth onwards, some of which may be shared on social media sites. Some parents even set up accounts for their infants in their own names on these sites, so that their social media profiles are established at birth (Ammari et al., 2015; Holloway et al., 2013).

As children grow, parents can track their health, development and physical activities using apps. Children may be given wearable devices such as the LeapFrog LeapBand™, a digital wristband connected to an app that encourages children to be physically active in return for providing them with the opportunity to care for virtual pets. Children often begin to use mobile digital devices in infancy – particularly smartphones and tablet computers (Holloway et al., 2013). Via their use of these technologies, internet corporations can begin to collect information on their online browsing and searching habits. Many thousands of apps for mobile devices have been developed with infants and pre-schoolers as their target audience. Such apps also

routinely collect personal information about their juvenile users, including their geolocation, age, gender and the ways in which they use the app. Digitized toys such as Mattel's 'Hello Barbie' doll, equipped with speech recognition software and Wi-Fi, encourage children to interact with them (Timms, 2015).

When children enter the formal education system, these forms of dataveillance and datafication are complemented by many others. The monitoring of children's educational progress and outcomes using software is now routinely undertaken in many schools, as are their movements around the school. In the UK, the majority of schools have CCTV cameras that track students, and many use biometric tracking technologies such as RFID (radio frequency identification) chips in badges or school uniforms and fingerprint or retina scanning to identify children and monitor their movements and purchases at school canteens (Taylor, 2013). More subtly, the details of children's education are routinely captured in databases. Notably, the UK's National Pupil Database contains detailed data on over 7 million British schoolchildren from 2002 onwards, constituting one of the largest educational datasets in the world. These linked datasets, combined with databases of information from further and higher education, enable individual pupils to be monitored throughout the educational life course. In the US, under initiatives introduced by the Obama administration, children are monitored not only by commercial companies when they log into software, but also their personal health, wellbeing and education details are tracked by government agencies from early infancy until they start work. The idea is to use these big datasets to contribute to educational policy. The Education Department lists hundreds of questions that it asks states to answer about each child in the public education system, including about their mental health and social skills (Simon, 2014).

Newer digital techniques of dataveillance are beginning to proliferate through schools, marking a shift from the 'surveillance school' (Taylor, 2013) associated with CCTV to 'dataveillance schools' that involve the routine collection and analysis of children's data (Williamson 2017). In the early years of primary school, the behaviour-monitoring app 'ClassDojo' has been used by over 3 million teachers with 30 million pupils in 180 different countries. 'ClassDojo' constitutes a kind of behavioural surveillance of the child, encouraging teachers to award or deduct points in relation to positive character indicators. It converts behavioural data into a form of value – in the shape of Dojo points – that children can themselves exchange in the digital economy of the classroom while making data collection and visualization into a form of gamified 'pleasurable surveillance' (Whitson, 2013).

Outside the classroom, it is increasingly possible to conduct forms of dataveillance on children through physical activity monitors. On the playing field or in the gymnasium, for example, teachers can generate data on children's physical activity using tools such as 'FitnessGram', 'Sqord' and 'Zamzee' that are based on the

technologies used by self-trackers. 'Zamzee', the 'game that gets kids moving', consists of a wearable 'meter' device to 'measure the intensity and duration of physical activity', an online 'motivational website' featuring challenges and lesson plans and 'group analytics' to enable educators and school administrators to 'track individual and group progress with real-time data.' The strapline for the product is 'Motivate. Measure. Manage'. These body surveillance devices project an optimal form of fitness and wellbeing into a kind of pleasurable body pedagogy that conveys normal expectations and moral codes about health (Lupton, 2015a; Williamson, 2015).

One of the most significant forms of dataveillance in education is 'learning analytics'. Learning analytics platforms are designed to mine data about learners as they go about educational tasks and activities in real time, and to provide automated predictions of future progress that can then be used as the basis for intervention and pre-emption (Siemens, 2013).

Notably, Pearson, the world's largest educational publisher and e-Learning provider, has partnered with Knewton, a major learning analytics provider, to power its digital content for the schools market. Knewton's 'Adaptive Learning Platform' is described on the company website as enabling 'real-time assessment of the individual'. It enacts techniques such as 'algorithmic assessment norming at scale', 'ground-breaking machine learning algorithms' and prescriptive analytics 'recommender systems'. These learning analytics platforms mobilize the data captured from students for future prediction of learning progress, and even prescription of educational pathways.

Although most learning analytics platforms are aimed at monitoring academic progress, emerging forms of 'emotional learning analytics' extend their capacity to capture real-time data about children's affective and non-cognitive learning experiences. Emotional learning analytics make extensive use of psychometrics, sentiment analysis and natural language processing. They employ other data sources such as face cams, video, eye tracking, skin temperature and conductivity to enable the automatic detection, assessment, analysis and prediction of the emotional state of learners through measurable behavioural indicators and other proximal indicators of learning on a real-time basis (Montero and Suhonen, 2014; Rientes and Rivers, 2015). These approaches to emotional learning analytics make children's behaviours, emotions and non-cognitive experiences possible to monitor through techniques of dataveillance, at the same time as conventional learning analytics appear to conduct a real-time dataveillant diagnostics on their cognitive performances, and as activity monitors measure their physical exertions. The body, mind and brain of the child are all subjects of an increasingly surveillant gaze, rendered visible in numbers and visualizations for inspection (whether by human specialist or technical system).

Risks and privacy harms

Many issues and concerns are raised by the proliferation of digital technologies directed at the datafication and dataveillance of young children. It is important to recognize that voluntary self-surveillance provides benefits for those who participate. Children can gain pleasure, enjoyment or reassurance from practices of datafication and dataveillance. For children who choose to engage in self-surveillance and social surveillance, such practices may contribute to processes of selfhood and identity. They can find self-surveillance helpful or productive as a means to exercise control over their lives and engage in self-improvement (Lupton, 2016). They may enjoy sharing personal details about themselves with others on social media sites as part of self-presentation and the promotion of social relationships (Marwick, 2012; Sauter, 2014). These practices can contribute to the ways in which 'children exercise rights to information, education and participation', and access, understand and participate in digital media (Livingstone, 2016: 10).

Dataveillance carried out on children by others, as well as mutual social surveillance, can also contribute positively to children's close relationships and wellbeing. For those people who are monitoring features of the children in their lives using dataveillance technologies, the generated information can assist their caring strategies. In this context, intimate surveillance can be important to the formation of identities as loving and committed parents, family members or friends, or their professional identities as caregivers, teachers or healthcare providers (Finn, 2016). In this sense, dataveillance can be understood as a new form of ethical care provision. In participating in dataveillance, therefore, both children and adults are conforming to idealized neoliberal notions of the entrepreneurial subject who takes responsibility for managing and optimizing her or his life (or those for whom one has caring responsibilities) (Lupton, 2016).

However, the possible negative ramifications of the datafication and dataveillance of children and their challenge for children's rights also need to be highlighted. As a growing number of critics are beginning to argue (Lyon and Bauman, 2013; Robinson et al., 2014; Rosenblat et al., 2014), people's life chances and access to opportunities are increasingly becoming shaped by the types of social sorting afforded by dataveillance. People have few opportunities to challenge the inferences and predictions that are made by algorithmic calculations. They often have little knowledge about how corporations are exploiting their personal details and using them to construct detailed profiles on people used for decisions about their access to employment, insurance, social welfare, special offers and credit (Crawford and Schultz, 2014).

Given that a multitude of details are now collected on many children from pre-birth onwards and stored in digital databases, these uses of personal data may well have profound implications for the current generation of children. Such practices inscribe

children within an ever-intensifying network of visibility, surveillance and normalization, in which their behaviours and bodies are continually judged and compared with others. One issue relates to the ways in which children come to be understood and portrayed via the algorithmic knowledges that such practices generate about them. The apparently scientific neutrality of digitized quantification of children's attributes obscures the reductionism that such processes inevitably produce. In any mode of information-gathering, certain features are ignored or neglected, while others are brought to the fore. Rendering children's behaviours, qualities and bodies into digital data, and relying principally on these data when making important assessments, judgements or inferences about them, may delimit what can be known about them and how they might be treated as a result. What is considered knowable or calculable about children and their lives becomes the outcome of the digital device and its software.

Children are configured as algorithmic assemblages as the result of these practices, with the possibility that their complexities, potentialities and opportunities may be circumscribed. They are encouraged to view and compare themselves with others using these these assemblages from very early in their lifespans. They become 'calculable persons' who are the subject of calculations performed by others (and by other digital things) but are also enabled to think about, calculate about, predict and judge their own activities and those of others (Rose, 1999). These calculating children are both calculated and metricized as data traces, but also encouraged to calculate about themselves through encountering their own data, albeit data that has been collected, prepared and presented for them through techniques of analysis and visualization (Williamson 2017).

Thus, for example, learning analytics platforms appear to displace the embodied expert judgement of the teacher to the disembodied pattern detection of data analytics algorithms. Performing such analysis depends not just on surveillance of the individual, but on massive dataveillance of millions of data subjects to generate the kinds of big databases from which accurate predictions are made by comparing individuals against norms derived algorithmically from the masses. Despite their huge volume, learning analytics platforms have been queried for their potential to sort and filter students according to the norms and assumptions built in to proprietary algorithmic systems by their designers (Hope, 2015). A significant risk that children's opportunities might be narrowed by the assumptions encoded in algorithmic processes is raised by such techniques.

Via datafication, information about children's bodies and behaviours becomes rendered into a form of biocapital, a digital data mode of commercially exploiting human embodiment (Lupton, 2016). As we have shown, recruiting children and their parents as contributors to the unpaid digital labour workforce by such means begins very early in their lives. The use of data dashboards and other forms of data

visualization in educational settings also makes data about children into a form of value that can be exchanged by them for rewards such as upgrades and personalized features, transforming classrooms into little digital economies and calculative spaces where personal data has exchange value and utility.

Across the diverse range of methods for datafying children, their rights are rarely considered. Critics of the increasingly prevalent forms of datafication and dataveillance of citizens have pointed to the erosion of privacy to which such practices contribute, and the increasing power differentials that they facilitate. There are now significant ramifications for people's rights to data privacy, potential privacy harms and security issues arising from these new ways of collecting and using personal information (Solove, 2006). In addition to the covert modes of dataveillance on the part of internet corporations and national security agencies outlined earlier, data breaches or data leaking of large datasets owned by corporations are common. Hacking events for malicious or cyber-criminal purposes occur with regularity, often revealing very private details about individuals (McCarthy, 2013; Rosenzweig, 2012).

These practices affect children as well as adults. It can be difficult to verify children's ages on online sites and apps, and their data are often treated in similar ways to those of adults. Legislation such as the US Children's Online Privacy Protection Act has been instituted to restrict the collection of children's personal data online. In response, social media sites often limit membership to those aged 13 and over. However, it is relatively easy on many sites simply to use a false birthdate to create an account (boyd et al., 2011), while others do not request such information. Furthermore, such legislation cannot protect children from hacking events and data breaches, nor from their parents' or other adults' choices to share details about them online. Indeed, it has been found that parents often help under-age children to join social media sites (boyd et al., 2011).

Various data breaches specifically related to young children have come to light in recent years. It has been demonstrated that online educational platforms for children often do not sufficiently protect the data security and privacy of users' personal details. One example is the hacking of VTech, a Hong Kong company that manufactures digital baby monitors and educational toys for infants and young children. Its data archives were hacked in November 2015, compromising the details of over 5 million customer accounts and their related profiles of child users of the devices. The stolen data included children's names, birth dates, mailing and email addresses (Peterson, 2015). Various stories about hackers gaining access to digital baby monitors and speaking to infants directly through these devices have also received media attention (Owens, 2015). The 'Hello Barbie' toy not only records details of the children's words in the toy companies' database, but also poses opportunities for hackers to access these data (Timms, 2015). Concerns have been raised about how Google uses the student data entered into their

suite of school-based software, Google Apps for Education, used by many schools in the UK, US and Australia (EFF, 2015).

Parents and schools are only beginning to consider the implications of generating reams of often very personal and private data about children for the children themselves, either currently or in the future. Given that many parents begin to construct a public digital profile for their children before they are even born, research suggests that they have not yet considered the implications for their children of divulging information about them online, including privacy risks and security issues (Duggan and Lehnhart, 2015; Lupton and Pedersen, 2016). When parents are using digital forms of monitoring their children, they are generating further streams of information that other agencies could potentially access. As children grow older, they may find the intimate surveillance conducted on them by their parents intrusive. This is evident from teenagers' responses to parents observing their activities on social media sites such as Facebook (West et al., 2009). As they begin to use social media themselves and make connections with each other, children must also confront the implications of the types of participatory or social surveillance they exercise on each other via social media (Madden et al., 2013).

Educational systems are struggling to come to terms with dealing with these digital rights issues, and to inform parents, students and teachers about how best to protect children's personal and private information (Polonetsky and Jerome, 2014; Singer, 2015a, 2015b). Several American states have passed bills intended to bolster protection of school students' information generated by online educational programs (Singer, 2015a). The Future of Privacy Forum (2016) has published several documents concerning this issue. One of its reports, *Student Data: Trust, Transparency and the Role of Consent* (Polonetsky and Jerome, 2014), describes the major issues concerning the use of students' personal data in schools, as well as issues of age verification and consent. The Forum has also produced *A Parents' Guide to Student Data Privacy* as a document for school students and their parents to learn about the issues, and to use as a source for communicating with schools. It was involved in designing the Student Privacy Pledge (2016), effective from 1 January 2015 and endorsed by US President Obama. This Pledge includes the signatures of over 200 leading educational technology companies as well as major internet companies such as Apple, Google and Microsoft, agreeing to safeguard the privacy of school students' personal information in their corporate practices.

Speaking for themselves: data and children's rights

Internet studies scholars have only just begun to confront the issue of children's rights in the digital age. The field of childhood studies has sought to engage with key issues in children's rights, but little scholarship in this field has devoted attention to data privacy

issues. As childhood theorist Lee (2001: 93) has argued, one of the central concerns emerging from the UN CRC has been that children are enabled to 'speak for themselves'. This acknowledges that 'adults cannot always be relied upon to speak on children's behalf, and that adults' interests do not always coincide with those of children.' Similarly, although perhaps surprisingly, the dominant discourse around digital data has concerned the idea that data can 'speak for themselves', free from human bias, positionality or predetermined framing.

The issue of children's digital rights in relation to datafication and dataveillance needs to be situated in the context of both of these contentions. Both have been critiqued. For example, Livingstone (2016) notes that the children's rights discourse has tended to favour a normative late-modern vision of participatory democracy that assumes positive freedoms (or positive rights) to information and engagement. Additionally, Lee (2001) claims that the UN CRC provides an attenuated view of the child's voice, insofar as it applies the right of free expression only to those children who are 'capable of forming' their own views. He acknowledges that 'age and maturity' will 'weight' the significance that is subsequently given to what they say. In response to the common assumption that digital data speak for themselves, critical data studies scholars have highlighted that data are never entirely impartial, neutral or objective. Their generation and interpretation always involve particular viewpoints, ideological frameworks, forms of disciplinary expertise, as well as the values, assumptions and biases of those who collect and analyse them (Andrejevic, 2014; Kitchin, 2014; Lupton, 2015b; van Dijck, 2014).

With many of the child surveillance data assemblages detailed above, data that speak for themselves are positioned in ways that override the rights of children to speak for themselves. Educational applications such as 'ClassDojo' translate children's classroom behaviours into visualized behavioural profiles and timelines that can be transmitted to parents for inspection in the home. Learning analytics and adaptive learning platforms make data-processing algorithms and predictive analytics technologies into key techniques for the personalization of education, therefore erasing children's own embodied experiences and voices from decision-making processes about their learning.

Rather than engaging children in their right to involvement in decisions about important matters that affect their lives, many analytics systems appear to distribute decision-making to automated, proprietary systems where children have little opportunity for involvement in the handling or use of their personal data. The collection, processing and dissemination of children's data may be intrusive, as it is used to inform decision-making by others that might have a significant impact on children's own lives. Yet these children surveillance data assemblages by no means speak solely for themselves. Rather, they consist of a range of embedded forms of

knowledge and expertise, norms and values that originate with their designers and are encoded in the data the tools provide. For example, the field of learning analytics is largely underpinned by cognitive science theories of learning that determine how the platforms are designed to detect patterns that indicate learning. Likewise, physical activity trackers designed for use by children are based on particular biomedical explanations of the body, twinned with norms derived from governmental and commercial agendas around health and fitness that determine how the devices classify the child's health status and wellbeing.

In many approaches to the datafication and dataveillance of children, the embodied and subjective voices of children are displaced by the supposed impartial objectivity provided by the technological mouthpieces of data. Data are positioned to provide a more detailed and manageable account of who children really are, free from the messiness of dialogic deliberation and freedom of expression. These data are also often considered to provide 'actionable' forms of intelligence and insights that cannot be gleaned from human observation and experience. It is notable, for instance, that in the educational context, the collection and analysis of children's data has been associated with the discourse of 'personalization', a term previously used to refer to educational initiatives designed to be more 'learner-centred', and acknowledging of children's own perspectives on their learning as well as their interests and needs (Selwyn, 2016). In this sense, the child-centred emphasis of personalization, like that of children's rights discourses, is currently being challenged by a data-centred focus on the collection of intimate information that can speak on behalf of children.

Conclusion

We have identified and explored a tension here between child surveillance data assemblage and child data rights assemblage, where the latter may be understood as an ideal assemblage consonant with the full provision of children's rights in relation to digital technologies. There remains little evidence that specific instruments to safeguard children's rights in response to dataveillance have been developed or implemented. For Lee (2001: 116), children's rights instruments such as the UN CRC offer the potential for a new assemblage involving children. This is 'an assemblage that protects children while not claiming complete ownership of them', where 'the teacher changes from a powerful and commanding leader to a facilitator of learning' and 'the parent has to learn to balance the privacy of childhood within the home with childhood's new openness to the world of consumption and mediated images.' Children are perceived as actors with rights who might speak for themselves. In contrast, the data assemblages produced by practices of datafication and dataveillance tend to emphasize the enumeration of information about children and speak on their behalf. While the UN CRC has become successful in involving children as individuals with rights, there is little to suggest that

an assemblage that combines children, their rights and practices of digital dataveillance (the child-surveillance-data-rights assemblage) yet exists. New kinds of children's rights instruments that might combine with and mitigate the potential risks and harms of data surveillance assemblages involving children remain an urgent priority for policy development.

References

Albrechtslund A and Lauritsen P (2013) Spaces of everyday surveillance: Unfolding an analytical concept of participation. *Geoforum* 49: 310–16.

Ammari T, Kumar P, Lampe C and Schoenebeck S (2015) Managing children's online identities: How parents decide what to disclose about their children online. In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15).* ACM Press, 1985–904.

Andrejevic, M (2014) The big data divide. *International Journal of Communication* 8: 1673–89.

Bellman M and Vijeratnam S (2012) From child health surveillance to child health promotion, and onwards: A tale of babies and bathwater. *Archives of Disease in Childhood* 97(1): 73–7.

boyd d, Hargittai E, Schultz J and Palfrey J (2011) Why parents help their children lie to facebook about age: Unintended consequences of the 'children's online privacy protection act'. *First Monday* 16. Available at: http://journals.uic.edu/ojs/index.php/fm/article/view/3850

Crawford K and Schultz J (2014) Big data and due process: Toward a framework to redress predictive privacy harms. *Boston College Law Review* 55(1): 93–128.

Duggan M and Lehnhart A (2015) *Parents and Social Media*. Washington, DC: Pew Research Center. Available at: www.pewinternet.org/2015/07/16/parents-and-social-media/

EFF (Electronic Frontier Foundation) (2015) Google deceptively tracks students' internet browsing, EFF says in FTC complaint. 1 December. Available at: www.eff.org/press/releases/google-deceptively-tracks-students-internet-browsing-eff-says-complaint-federal-trade

Elmer G (2003) A diagram of panoptic surveillance. *New Media & Society* 5(2): 231–47.

Finn M (2016) Atmospheres of progress in a data-based school. *Cultural Geographies* 23(1): 29–49.

Future of Privacy Forum (2016) *About K-12 Education*. Available at: https://fpf.org/issues/k-12-education/

Gane N (2012) The governmentalities of neoliberalism: Panopticism, post-panopticism and beyond. *The Sociological Review* 60(4): 611–34.

Holloway D, Green L and Livingstone S (2013) *Zero to Eight: Young Children and Their Internet Use*. London, UK: EU Kids Online. Available at: http://eprints.lse.ac.uk/52630/1/Zero_to_eight.pdf

Hope A (2015) Foucault's toolbox: Critical insights for education and technology researchers. *Learning, Media and Technology* 40(4): 536–49.

Jenks C (2005) *Childhood: Critical Concepts in Sociology*. New York: Routledge.

Kitchin R (2014) *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences.* London, UK: Sage.

Leaver T (2016) Born digital? Presence, privacy, and intimate surveillance. In: Hartley J and Qu W (eds) *Re-orientation: Translingual, Transcultural, Transmedia*. Shanghai: Fudan University Press, 149–60.

Lee N (2001) *Childhood and Society: Growing Up in an Age of Uncertainty*. Maidenhead, UK: Open University Press.

Levy K (2015) Intimate surveillance. *Idaho Law Review* 679. Available at: www.uidaho.edu/law/law-review/articles

Livingstone S (2016) Reframing media effects in terms of children's rights in the digital age. *Journal of Children and Media* 10(1): 4–12.

Longhurst R (2009) YouTube: A new space for birth? *Feminist Review* 93: 46–63.

Lupton D (2013) *The Social Worlds of the Unborn*. Houndmills, UK: Palgrave Macmillan.

Lupton D (2015a) Data assemblages, sentient schools and digitised health and physical education (response to Gard). *Sport, Education and Society* 20(1): 122–32.

Lupton D (2015b) *Digital Sociology*. London, UK: Routledge.

Lupton D (2016) *The Quantified Self: A Sociology of Self-tracking*. Cambridge, UK: Polity Press.

Lupton D and Pedersen S (2016) An Australian survey of women's use of pregnancy and parenting apps. *Women and Birth*. Available at: www.ncbi.nlm.nih.gov/pubmed/26874938

Lupton D and Thomas GM (2015) Playing pregnancy: The ludification and gamification of expectant motherhood in smartphone apps. *M/C Journal* 18. Available at: http://journal.media-culture.org.au/index.php/mcjournal/article/viewArticle/1012

Lyon D and Bauman Z (2013) *Liquid Surveillance: A Conversation*. Oxford, UK: Wiley.

Madden M, Lenhart A, Cortesi S, Gasser U, Duggan M, Smith A and Beaton M (2013) *Teens, Social Media, and Privacy*. Washington, DC: Pew Research Center. Available at: www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/

Marwick A (2012) The public domain: Social surveillance in everyday life. *Surveillance & Society* 9(4): 378–93.

Mccarthy M (2013) Experts warn on data security in health and fitness apps. *British Medical Journal* 347. Available at: www.bmj.com/content/347/bmj.f5600

Montero CS and Suhonen J (2014) Emotion analysis meets learning analytics: Online learner profiling beyond numerical data. In: *Proceedings of the 14th Koli Calling International Conference on Computing Education Research*. Koli, Finland: ACM Press, 165–9.

Owens C (2015) Stranger hacks family's baby monitor and talks to child at night. *The San Francisco Globe*. Available at: http://sfglobe.stfi.re/2016/01/06/stranger-hacks-familys-baby-monitor-and-talks-to-child-at-night/?sf=zpbnxl

Peterson A (2015) Toymakers are tracking more data about kids – leaving them exposed to hackers. *The Washington Post*, 30 November. Available at: www.washingtonpost.com/news/the-switch/wp/2015/11/30/toymakers-are-tracking-more-data-about-kids-leaving-them-exposed-to-hackers/

Polonetsky J and Jerome J (2014) *Student Data: Trust, Transparency and the Role of Consent*. Future of Privacy Forum. Available at: https://fpf.org/wp-content/uploads/FPF_Education_Consent_StudentData_Oct2014.pdf

Raley R (2013) Dataveillance and countervailance. In: Gitelman L (ed.) *'Raw Data' is an Oxymoron.* Cambridge, MA: MIT Press, 121–45.

Rientes B and Rivers B (2015) *Measuring and Understanding Learner Emotions: Evidence and Prospects*. Bolton, UK: University of Bolton.

Robinson D, Yu H and Rieke A (2014) *Civil Rights, Big Data, and our Algorithmic Future*. Robinson + Yu. Available at: http://bigdata.fairness.io/wp-content/uploads/2014/09/Civil_Rights_Big_Data_and_Our_Algorithmic-Future_2014-09-12.pdf

Rose N (1999) *Powers of Freedom: Reframing Political Thought.* Cambridge, UK: Cambridge University Press.

Rosenblat A, Wikelius K, boyd d, Gangadharan SP and Yu C (2014) *Data and Civil Rights: Health Primer*. Data & Society Research Institute. Available at: www.datacivilrights.org/pubs/2014-1030/Health.pdf

Rosenzweig P (2012) Whither privacy? *Surveillance & Society* 10(3/4): 344–7.

Sauter T (2014) 'What's on your mind?' Writing on Facebook as a tool for self-formation. *New Media & Society* 16(5): 823–39.

Selwyn N (2016) *Is Technology Good for Education?* Cambridge, UK: Polity.

Simon S (2014) Big brother: Meet the parents. *Politico*. Available at: www.politico.com/story/2014/06/internet-data-mining-children-107461.html

Singer N (2015a) Tools for tailored learning may expose students' personal details. *The New York Times*, 30 August. Available at: www.nytimes.com/2015/08/31/technology/tools-for-tailored-learning-may-expose-students-personal-details.html?_r=0

Singer N (2015b) Uncovering security flaws in digital education products for schoolchildren. *The New York Times*, 8 February. Available at: www.nytimes.com/2015/02/09/technology/uncovering-security-flaws-in-digital-education-products-for-schoolchildren.html

Student Privacy Pledge (2016) Available at: http://studentprivacypledge.org/

Taylor E (2013) *Surveillance Schools: Security, Discipline and Control in Contemporary Education.* Houndmills, UK: Palgrave Macmillan.

Thomas GM and Lupton D (2015) Threats and thrills: Pregnancy apps, risk and consumption. *Health, Risk & Society* 17(7-8): 495–509.

Timms P (2015) Hello Barbie: Wi-Fi enabled doll labelled a bedroom security risk. Available at: www.abc.net.au/news/2015-11-27/wi-fi-enabled-hello-barbie-doll-raises-security-concerns/6981528

UN (United Nations) (1989) *Convention on the Rights of the Child*. Geneva: UN, Office of the High Commissioner for Human Rights.

van Dijck J (2014) Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society* 12(2): 197–208.

West A, Lewis J and Currie P (2009) Students' Facebook 'friends': Public and private spheres. *Journal of Youth Studies* 12(6): 615–27.

Whitson J (2013) Gaming the quantified self. *Surveillance & Society* 11(1/2): 163–76.

Williamson B (2015) Algorithmic skin: Health-tracking technologies, personal analytics and the biopedagogies of digitized health and physical education. *Sport, Education and Society* 20(1): 133–51.

Williamson B (2017) Calculating children in the dataveillance school: personal and learning analytics. In E Taylor and T Rooney (eds) *Surveillance Futures: Social and ethical implications of new technologies for children and young people*, 50-66. London: Routledge.