The Routledge Companion to Digital Media and Children

Lelia Green, Donell Holloway, Kylie Stevenson, Tama Leaver, Leslie Haddon

Balancing Privacy

Publication details
Tama Leaver
Published online on: 28 Oct 2020

How to cite :- Tama Leaver. 28 Oct 2020, Balancing Privacy from: The Routledge Companion to Digital Media and Children Routledge
Accessed on: 21 Nov 2023

Please scroll down for document

Full terms and conditions of use: https://www.routledgehandbooks.com/legal-notices/terms

This Document PDF may be used for research, teaching and private study purposes. Any substantial or systematic reproductions, re-distribution, re-selling, loan or sub-licensing, systematic supply or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The publisher shall not be liable for an loss, actions, claims, proceedings, demand or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.
22

BALANCING PRIVACY

Sharenting, Intimate Surveillance, and the Right to Be Forgotten

Tama Leaver

Introduction

In early 2020, the daughter of a prominent Instagram influencer used an anonymous account to post to the Reddit forum ‘Am I the Asshole?’ where posters describe a personal situation and ask other users to judge whether they were in the right or wrong. In her message, the original poster (OP) described how she had ordered custom-made hoodies with various messages printed on them, including “no photos”, “I do not consent to be photographed”, “respect my privacy”, and “no means no” (FinallyAnonymous6, 2020). The OP describes wearing this hoodie, and providing her younger sister with one for the same reason, to prevent her influencer mother taking photos of her and sharing them on social media. The OP made it clear that she had requested her mother stop sharing photos of her a number of times, and made it explicitly clear that she did not consent to any images being posted online. As her mother did not respect the OP’s request, she had begun wearing the hoodie in her home, to family events, and anywhere her mother might be taking photos, to deliberately interrupt her mother’s photography and online sharing. This upset her mother, who argued that featuring her daughters on Instagram was part of the way the family made their income. The post struck a chord on Reddit, attracting more than 3,500 responses before comments were locked. The vast majority of responses commended this as a very effective and justified tactic, and many agreed that the OP’s mother urgently needed to respect her desire for privacy. Beyond this anecdote, which demonstrates a very satisfying display of children’s digital literacy in negotiating their privacy boundaries, this story also points to a number of related questions. Should parental influencers share photos of their children, within what boundaries, and how might influencers model behaviour for other parents? More broadly, while ‘sharenting’ – parents sharing images of their children online – is incredibly widespread, what are the ongoing privacy implications of this practise? Beyond the level of images and immediate public visibility, what happens to the underlying data generated when images and media featuring young people is shared on various platforms? Moreover, do children today have a right to be forgotten online, as their digital footprints potentially last forever? Ultimately, this chapter pursues these questions to ask how exactly the digital communication and sharing of and by parents about their children can be balanced with children’s rights to privacy both in the present and, more challengingly, in the future.


Tama Leaver

Child and Parent Influencers: Inadvertent Role Models?

Ryan’s ToysReview, which has subsequently rebranded as Ryan’s World, is the most profitable YouTube channel in the world, featuring a nine-year-old boy, making an estimated $US26 million in 2019 from sponsored posts (Spangler, 2019). Since March 2015, Ryan Kaji has been featured in toy unboxing videos in which he euphorically unwraps and examines new toys, all shared on YouTube; he was an instant hit, so much so that within two years his parents left their own jobs to focus exclusively on managing Ryan’s YouTube channel and the commercial opportunities it led to. While Ryan’s parents keep some details of his life private (his exact birthday, for example), he has nevertheless grown up on YouTube and his immense profitability highlights just how successful child influencers can be if a certain level of intimacy and familiarity is built with audiences, usually at the cost of a child influencer’s privacy.

In the Australian context, one of the most well-known child influencers is Pixie Curtis, who is on Instagram as Pixie’s Bows. Pixie is the daughter of CEO and PR executive Roxy Jacenko who, herself, is an influencer of considerable impact, with over 250,000 followers. Pixie has a more modest 95,000 followers, but commands huge reach with parents and young girls. Jacenko has been criticised publicly and in many comments for over-exposure of Pixie who has been online since she was very young (Fitch, 2017). Pixie now has a successful brand of hair products – Pixie’s Bows – and has begun a modelling career at the age of seven. While Jacenko’s approach to Pixie has been critiqued publicly, Jacenko has, at least, articulated a clear vision of Pixie’s presence online, including ensuring that any profits made go directly into a fund for Pixie’s future and education. Even if others disagree, it is certainly the case that Jacenko has considered and articulated a clear position on her daughter’s online presence and the trade being made in exchanging privacy for public visibility (Archer, 2019). Pixie is an example of what Abidin (2015) calls a ‘micro-microcelebrity’, that is, a second generation influencer whose parents are already in the social media spotlight and whose childhood is shaped, in part at least, as part of their parents’ online presence, and then fairly swiftly as an influencer in their own right. As Abidin notes, micro-microcelebrities provoke some of the most difficult questions around child influencers, including whether parents are effectively exploiting the free labour of their children, as well as more immediate questions of what privacy is really available to a child whose life and lifestyle is documented on social media for profit from birth, if not before.

While children are almost always a core part of what any parental influencer talks about, there are many different approaches to balancing the visibility and privacy of children on social media (Blum-Ross & Livingstone, 2017). Anna Whitehouse is a long-time parental influencer and flexible working advocate who blogs, and is on Instagram, as Mother Pukka; Whitehouse is one example of someone explicitly modelling best practice in terms of sharing images and information about her children. In a long blog post (also pointed to from her other social media presences), Whitehouse collates information from experts and scholarship, and reveals her own practices including: initially using pet names, and eventually just emoji, to refer to her children, protecting their real names; not revealing a host of specific information including their schools; and only photographing them, if at all, from behind or in a way that obscures their faces (Whitehouse, 2018). Moreover, on Instagram and elsewhere, Whitehouse has publicly engaged in extensive dialogue with her followers and other parental influencers about children’s privacy, inviting her followers to consider and perhaps update their own practices.

Parental and child influencers are on the front lines of social media. The practices deployed by influencers are often adopted as norms by other users. Ryan Kaji and Pixie Curtis represent one end of a spectrum where their presence online is substantial and privacy has been deliberately traded for commercial success. Anna Whitehouse and her children are toward the other end of the spectrum,
participating in parenting discussions while modelling a more privacy-centred approach in including, but not explicitly depicting, her children.

Sharenting: Ultrasounds and Beyond

Increasingly, a child’s first image online precedes their actual birth. Sharing ultrasound images has become a rite of passage; posting the 12- or 20-week prenatal ultrasound images on Facebook or Instagram is now a very common way to reveal a pregnancy across the Western world (Lupton, 2013). Sharenting – a portmanteau of the words share and parenting, conventionally referring to parents sharing images and videos of their kids online – is thus a practice that new parents often start enacting even as they attempt to prepare for all the other new challenges parenthood can entail. Moreover, as actors, sportspersons, and other celebrities share their prenatal ultrasounds with descriptions such as ‘his first photo!’, they normalise a process of sharing and naming visualisations of the unborn on social media (Seko & Tiidenberg, 2016). The choice to not share increasingly seems at odds with the norms and social expectations of pregnancy and (preparing for) parenthood in the era of social media platforms.

In examining over 10,000 images and videos publicly shared on Instagram using the #ultrasound hashtag over a period of three months in 2014, Leaver and Highfield (2018) surfaced a range of practices in which ultrasounds were shared, from photos and scans of the ultrasounds themselves to excited selfies of mothers and couples heading to their first ultrasound scan, through to printed ultrasound images held in stylised poses to announce a pregnancy. In a qualitative coding, the authors found that of the prenatal ultrasounds publicly shared on Instagram, 34% of them had personally identifiable data and metadata such as the mother’s full name, the hospital or facility doing the scan, the mother’s date of birth, the estimated due date of the foetus, and so forth. While this metadata was usually visible as part of the image, not separate text in the image’s textual description, it is nevertheless a fairly trivial task for an algorithm to ‘read’ the visual text and incorporate it into Instagram’s metadata about that person. Moreover, as Facebook harnesses, connects, and indexes millions of data points and sources to better map their users, and better target advertising to them, it is entirely likely that such metadata not only informs advertising aimed at the expecting parents, but also that Facebook would start a profile for the foetus in question. Indeed, making the process even more seamless, commercial ultrasound machines today often come bundled with the Tricefy software that delivers all the images collected during an ultrasound scan and sends these as online links that can be shared directly with family or friends, or posted directly to Facebook or Instagram. It is notable, though, that when Leaver and Highfield (2018) collected their data, Instagram had relatively simple privacy options (accounts were either fully public or fully private). Since then, direct messaging and Stories (which disappear after 24 hours) have given parents more nuanced tools to share with specific audiences rather than the whole of Instagram’s userbase (Leaver et al., 2020). Yet, in February 2020, searching Instagram for #ultrasound still found 660,941 public posts, while the related hashtag #pregnancyannouncement also returned 574,633 public posts. Not all of these are ultrasound images, but a significant proportion are, as well as other visual devices to announce a pregnancy from a positive result on a pregnancy test to a pink or blue coloured cake purportedly revealing the sex of the foetus. If, as Kumar and Schoenebeck (2015) argue, new parents, and mothers especially, have to negotiate the desire other people have to see shared baby photos, this has to be weighed against a new parent’s own responsibilities to the child; the first ultrasound is thus not just the beginning of sharenting, but also when a parent’s ‘privacy stewardship’ of their child’s presence and data begins.

For parents, the question of whether or not to share images of their children online is not (just) based on the present and future privacy of their child, but is often also driven by a number
of other factors, including the expectation of other parents, friends, and family members who express clear desires to see newborn, baby, and growing up photos and, indeed, who may criticise new parents for any failure to share on social media (Damkjaer, 2018). For new parents, navigating the challenges of protecting their child’s privacy whilst also utilising the support and community Facebook can bring, for example, can be particularly paradoxical. In a study of new Australian mothers, for example, Chalklen and Anderson (2017) found that many were acutely aware of issues with children’s privacy online, but also found Facebook to be an extremely important source of support and networking with other new parents. These tensions were sometimes productive, leading to techniques for sharing but not identifying children, such as photos taken always from behind, being developed as norms within these support groups. Similarly, while some laws have come in to place to protect children’s data online, these laws often rely on parents as informed champions of their children’s privacy, which is not a role they are always able or willing to perform (Fox & Hoy, 2019; Steinberg, 2017). As children grow older, parents transition from being the exclusive decision-maker about sharing photos of their children online to a situation where children start exercising their voice and opinion about what should, and should not, be shared online. At times this can lead to ‘boundary turbulence’ in that the privacy expectations of children and their parents may not align, and difficult but important conversations can ensue (Lipu & Siibak, 2019). As children grow and usually start using their own social media accounts, their desire to shape their own identities and personality online can conflict with parental sharing, although in some contexts these conversations, too, can often be very productive with new boundaries and expectations emerging (Ouvrein & Verswijvel, 2019). However, young people’s experiences of sharenting can often be predominantly negative. A study of 817 Flemish adolescents with a roughly balanced gender split, for example, found that the vast majority found their parents’ sharenting practices ‘embarrassing and useless’ with only a small minority seeing any value in what their parents shared about them online (Verswijvel et al., 2019).

While negotiating different expectations of privacy on social media can be a confronting process, it is especially important as contemporary parents are often of an age where their own parents did not have to manage children’s social media and data traces in a networked world. Moreover, rather than parents just creating their children’s social media identities, as children become more active online they, too, may start posting about, and thus shaping, their parents as well. In the anecdote that began this chapter, the OP was not just resisting parental sharing, but in posting about her grievances she was also potentially shaping the online identity of her mother. These two-way streets serve as fruitful reminders that social media is actually almost always ‘co-creative’, in that, in so many instances when people post, they are contributing to the online presence of other people, a situation so readily visible in the realm of sharenting, but also inverted as children post about themselves and, over time, their families (Leaver, 2019). As co-creators, parents and children are thus in a dialogue about their own and others’ privacy online every time they post. Making that dialogue explicit, purposeful, and, ideally, agreed upon, will be part of family (and broader) negotiations in a world where most relations take place in complex intersecting combinations of physical and digital spaces.

**Wearables, Apps, and Sharable Data?**

While the debates and discussions about sharenting revolve around specific objects that can be relatively easily seen and located – this is, specific images and videos – the underlying level of data and metadata can be a lot harder to define, locate, or easily understand where it is generated, what is captured, what is stored, for how long, where, and under what control, including the big question of who owns that data. While data, and big data in particular, is surrounded by a mythology that big data leads to big answers, the processes and circumstances by which this
might happen are often, at best, deeply unclear (boyd & Crawford, 2012). Moreover, the generation of data about children may, in fact, be a by-product of an app, device, platform, or tool that is being used with the best of intentions to benefit children.

The Owlet ‘Smart Sock’ is an infant wearable device – that is, a device worn by an infant that collects certain health and metabolic information and transmits that to a device or platform – that provides parents with information about the blood oxygen levels, heart rate, and movement of a sleeping infant. This information is relayed to the cloud via a Bluetooth base station, and then the resulting data is made available to parents as a series of indicators on a smart phone app, which uses a traffic light system of indicators (green all is okay, yellow action is needed, red immediate intervention needed) to either reassure parents or indicate something is wrong. The motto in most of the Owlet sales material is that it offers weary parents ‘peace of mind’ in being able to be aware of their infant’s health without having to physically enter the room to check (Leaver, 2017). Indeed, while many parents infer that the Owlet is a device to prevent Sudden Infant Death Syndrome (SIDS), the Owlet is not certified as a medical device, and in the fine print it warns that it, in fact, cannot prevent SIDS. The device has been the subject of warnings from the American Academy of Pediatrics (Bonafide et al., 2017; King, 2014), which notes that the Owlet and similarly wearables can both provide false warnings, needlessly distressing parents, but also falsely reassure at times when it should not, and in both cases this impacts negatively on a child and parents’ health. However, despite these limitations, the company behind the Owlet continually imply that their smart sock is a viable safety measure for infants, and have enlisted a large number of parental influencers, including celebrity parent influencers such as Katherine Heigl, to promote the Owlet on their social media presences (Leaver, 2017). The Owlet is an example of what Leaver (2015, p. 153) describes as “intimate surveillance”, that is, “the purposeful and routinely well-intentioned surveillance of young people by parents, guardians, friends, and so forth”. While the term intimate surveillance serves as a useful reminder that surveillance practices can often be motivated by care, the term is also unsettling since surveillance is often associated with more sinister uses. In terms of the Owlet, what is perhaps less clear, and possibly more sinister depending on your perspective, is the amount of data the company collects, stores, analyses, and then owns about each child who uses the infant wearable. Not only does Owlet Baby Care state that they own all data generated by the smart socks – that is, measurements of every heartbeat, breath, movement, and blood-oxygen level, all linked to an exact time, place, and name – but it is clear that the company see their future success in being able to aggregate all the data from various babies and extrapolate new knowledge from that data. In this respect, the Owlet is typical of new heath apps and devices which ostensibly have two real products; one is the device or app itself, but the other is the data they collect, which can be stored and analysed as a big data set and potentially generate new forms of knowledge, but also new forms of income for the Owlet Baby Care company (van Dijck & Poell, 2016). Indeed, in its promotional videos the Owlet company is quite transparent and seemingly excited about its big dataset of baby data, claiming it has “the largest data set about infant health and sleep and wellness and safety that’s ever been collected” (Owlet Baby Care, 2015). Yet, for parents who have purchased the Owlet smart sock for ‘peace of mind’, the amount of personal information and data about their child they have signed away is unlikely to be clear since this transaction is shrouded in Terms of Use and legal terminology that tired parents are unlikely to have the patience or time to read when they are searching for anything that might help with a baby’s often very disruptive early sleep routine. These are far from ideal circumstances in which to have, effectively, made quite an important decision about the privacy of children’s data.

Indeed, having enough information to judge which apps, platforms, and companies to trust is one of the biggest challenges for parents in managing their children’s images and data. Peekaboo Moments is one example of a bespoke app that seemingly offers a solution for
families wary of using bigger advertising-driven platforms. Instead, the Peekaboo Moments app ostensibly offers a secure way to share images and videos of children with a specific, private group in a fashion that is consistent with the ease of Facebook, but without the larger privacy questions. However, despite their sales pitch of being a safer and more secure way to share children’s media and data, this was, for a period of time at least, far from true. In early 2020 security researchers discovered that over 100 gigabytes of user data from the Peekaboo Moments app was publicly accessible on an unsecured website, exposing images and videos of babies and various forms of identifiable information, from email addresses to changes in a baby’s weight over time (Kirk, 2020). Security researchers report reaching out to the people running Peekaboo Moments with information about the breach, but did not hear anything back until stories ran in the media about the breach, which did then lead to Peekaboo Moments securing their data to prevent future unsecured access. However, security researchers noted that the data was likely to have been visible online for eight or nine months before the security problem was fixed. For parents trying to make informed privacy choices, the Peekaboo Moments app ostensibly appears to be a safer choice than Facebook or Instagram, but, as the breach reveals, the company’s actual security did not match the rhetoric of security they were selling parents. Trying to weigh the security and privacy credentials of the plethora of apps, services, and platforms out there is extremely difficult, while app designers are often more focused on growth and profit, and the resources put into privacy and security often do not match the sales pitch to parents.

The Right To Be Forgotten?

For almost as long as social media has existed, questions have arisen about the challenges posed by every online utterance simultaneously being a piece of media that does not, by default, ever disappear. More than a decade ago Mayer-Schonberger (2009) warned that the ability to be forgotten was being eroded and may disappear altogether, or become something of a luxury product only available to those rich enough to pay to purge their digital traces. For children, and parents trying to look after children’s digital traces, the challenge of social media permanence is even more problematic. As Eichhorn argues, being able to forget, and be forgotten, matters: “Despite its bad reputation, forgetting has a function. Forgetting can help one take risks, explore new identities, embrace new ideas; it can help one grow up” (Eichhorn, 2019, p. 142). In an era of digital communication and datafied childhoods, there is no guarantee that commercial platforms and networks will ever ‘forget’ anything (Lupton & Williamson, 2017; Mascheroni, 2018).

In 1989 The United Nations Convention on the Rights of the Child enshrined a number of rights for children, including a specific right to privacy:

1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation;
2. The child has the right to the protection of the law against such interference or attacks. (UNICEF, 1989)

While this right might have been clear 30 years ago, it is more important than ever today, but it is also less clear than ever exactly how this right should be interpreted and respected in a digital, networked society (Livingstone & Third, 2017). As children age, they clearly understand the value of their reputation, and how that reputation is visible online, but many often lack the tools and competencies to maintain control of their own reputation. While Google and many other platforms organise content by impact and interest rather than chronology, as Eichhorn (2019, p. 141) notes,
Stupid or embarrassing moments, which are simply part of growing up, hold consequences they did not hold in the past. The psychosocial moratorium – that once granted at least some adolescents a temporary pass on suffering the consequences of their actions – has eroded.

Childhood moments resurfacing and communicating different meanings, often many years after being shared, is an example of ‘context collapse’ in that the context for sharing stories, photos, and other information may be very different to the context in which these pieces are viewed and scrutinised (Davis & Jurgenson, 2014; Marwick & boyd, 2011). For young people, their entire futures are an unknown context where their digital traces may reappear in searches and other ways that were never envisaged when these seemingly harmless photos, videos, or anecdotes were initially posted online. In the era of Google, a right to privacy, or to be forgotten, is thus very difficult to achieve.

The prospect of children’s privacy becomes even more complicated when their data is considered; the data collected by the Owlet smart sock or Peekaboo Moments, as discussed above, reveals how little control or ownership children, or their parents, have when using certain devices and apps, even if they are specifically designed for children. While data might be ‘anonymised’ before being collated, stored, or analysed, re-identifying individuals is relatively easy for rich data sources given there are so many ways to cross-reference various stored data. Names are only one data point. In many cases, though, the question of harm or risk is important, and sometimes very few risks are obvious. Yet one of the real challenges in thinking about children’s right to privacy is that it is not just how their media or data is used today, but also in the future. If the Owlet company was purchased by a large health or insurance company in a decade or two, could the data from an infant smart sock actually reveal some sort of heart defect or weakness that would lead to that child being denied health insurance as an adult? This might seem fantastical, but it is exactly these sort of inferences that might be made from big data that gives this data its value. For OP, the daughter of an influencer parent who no longer wants to have her photographs shared as part of her mother’s social media output, a right to be forgotten might entail erasing every photo OP is featured in, but the practicalities of this are hard to fathom, and, as is obvious from this example, children’s images and data are deeply intertwined with the data and media of other people, from their family and friends, and beyond. Untangling one person’s media and data would be a daunting and complex challenge, but a challenge that is one of the few clear paths to actually respecting children’s right to privacy in a digital world.

Conclusion

Most adults struggle to find the time to pay attention to the Terms and Conditions of every app they download, and often feel ill-equipped to manage their own data and own privacy online (Leaver & Lloyd, 2015; Plunkett, 2019). When people become parents and are suddenly responsible for a vast array of things to do with their children, managing their newborn’s digital footprints, social media presence, and personal data pose challenges that often the generations before them did not have to wrestle with. Without precedents to draw from, moral panics in the media about screen time and online predators may potentially drown out the seemingly more banal but equally important information about helping young people manage their online presence and privacy (Green et al., 2019). Increasingly, everything from child welfare services to interactive toys harness, generate, store, and potentially share personal data about children (Holloway & Green, 2016; Redden et al., 2020), without necessarily providing any transparency around the use, storage, or ownership of that data. While privacy itself can be conceptualised quite differently (Quinn et al., 2019), it is clear that from sharenting on social media to the data gathered by a host of apps across the fields of health,
entertainment, and education, privacy is seen as a barrier, not a right, to the operation and profitability of apps, platforms, and the companies that own them. For parents today, attempting to ensure children have a right to privacy can be a time-consuming, exhausting, and confusing task, wading through Terms and Conditions on one hand, while, on the other hand, negotiating the desires of different groups from friends and family and over time children themselves, all with different opinions, about what photos, videos, information, and data should be shared, where, and with whom. Returning to the anecdote about OP and her ‘no photos’ hoodie, that particular tale has specific value in that it points to the deep tactical literacy of a young person who managed to intervene creatively to achieve privacy for herself and her sister, at odds with her mother’s wishes. If young people are going to have a right to privacy today or in the future, it is exactly this digital literacy and bold tenacity that is needed in the face of a system of platforms, digital media, and big data which currently consume and keep as much personal data and information as possible. Moreover, it is important that researchers and educators work to provide new avenues for personal and parental literacies in understanding and managing personal data, ideally beginning before parenthood altogether, equipping new parents with the tools to curate and then help educate their children in terms of their digital traces. For parents, balancing the current and future privacy of their children is no small task, but one that matters more than ever and will likely be most successful with children as partners in the process.

**References**


Balancing Children’s Right to Privacy


