Selected Papers of #AoIR2023:
The 24th Annual Conference of the
Association of Internet Researchers
Philadelphia, PA, USA / 18-21 Oct 2023

TOWARD A REVOLUTION IN AUSTRALIAN CHILDREN'S DATA AND PRIVACY

Tama Leaver
Curtin University

Kate Mannell
Deakin University

Gavin Duffy
Deakin University

Anna Bunn
Curtin University

Rebecca Ng
University of Wollongong

Xinyu 'Andy' Zhao
Deakin University

This panel combines four papers which focus in different ways on the question of children's data and privacy in the Australian context. All four are framed with children's right to privacy as a core concern, consistent with the UN Convention on the Rights of the Child as updated via the General Comment 25 on Child Rights in the Digital Environment. We examine four arenas where children's data is either extracted or occluded in ways that make it more difficult, if not impossible, for parents, carers and others to make informed choices about the data of very young children. As children begin to articulate their own ideas and privacy preferences, these studies highlight different understandings of privacy, and of trust in both people and technologies. Collectively, these papers can be read as arguing that we need nothing less than a revolution in the way children and responsible adults are informed about the way children's data is generated, captured, stored, and owned, as well as explicitly regulating who can profit from children's data, in which circumstances, and how transparent these processes must be.

Suggested Citation (APA): Leaver, T., Mannell, K., Duffy, G., Bunn, A., Ng, R., and Zhao, X. (2023, October 19). *Toward a Revolution in Australian Children's Data and Privacy.* Panel presented at AoIR2023: The 24th Annual Conference of the Association of Internet Researchers. Philadelphia, PA, USA: AoIR. Retrieved from http://spir.aoir.org.

The first paper, by Kate Mannell, ‘Where Does Children’s Data Go? Mapping the Data Broker Industry’, focuses on the way that large data broker companies collect data either about children, or can infer data about children from other datapoints, despite regulation preventing targeted collection of children’s data in Australia. The paper examines the broad range of activities brokers undertake, including selling data and also selling ways to target groups, including, for example, parents with young children. While Australia is undergoing privacy reform around brokers, this paper warns that likely regulation does not go far enough as it does not restrict inferred data, nor companies selling access to groups rather than just selling the aggregated data itself.

In the second paper, ‘Data and Privacy as a Social Relation’, Gavin Duffy focuses on the educational technology (aka edtech) market and examines young children’s understanding of their own data in relation to edtech used in schools. Challenging conventional understandings, this paper finds that children see data more in terms of ownership than necessarily being digital. Of equal interest, young children tend to trust the use of their data because of trust in teachers, inferring that if a teacher uses edtech, they implicitly endorse any data use around these tools.

The third panel paper, ‘Developing a Holistic Framework for Analysing Privacy Policies – A Child’s Rights and Data Justice Perspective’ by Anna Bunn, Rebecca Ng, Xinyu ‘Andy’ Zhao and Gavin Duffy addresses the fact that in the Australian context most existing frameworks and terms of use are not clearly readable to many people and thus this paper offers a framework evaluating four domains – readability, visual analysis, textual analysis and historical analysis – which can produce accessible understandings of existing terms of service. In doing so this framework is explicitly situated with children’s rights and data justice in mind.

In the final paper, ‘Unboxing Data and Privacy Via Young Children’s Wearables’, Tama Leaver extends existing walkthrough methods which have focused on apps by adding the dimension of unboxing which highlights the physical packaging and framing of wearable devices marketed as being for very young children. Using case studies of the Owlet Smartsock and Nurofen Feversmart monitor, this last paper demonstrates a complete absence of any information about children’s data or privacy on these wearables and argues that this lack signals a need for better standards in the packaging of any device which collects children’s data.

Cumulatively, the four papers that constitute this panel diagnose serious problems in the way that data about children is generated, signaled, legally framed and commercially situated. Collectively these papers argue that we need a revolution in the way children’s’ data is managed and that their right to privacy needs to be better protected both in the present and the future since data has no built in expiry dates. At a moment where there is a global appetite for better regulation of big platforms, the same push should encompass better privacy practices and regulation in both Australia and across the globe.

Acknowledgement

All papers in this panel, this research was supported by the Australian Research Council Centre of Excellence for the Digital Child through project number CE200100022.

WHERE DOES CHILDREN'S DATA GO? MAPPING THE DATA BROKER INDUSTRY

Kate Mannell
Deakin University

Introduction

Scholars have raised alarm about what the datafication of childhood might mean for children's rights (Lupton and Williamson, 2017) and some jurisdictions have begun working toward improved regulations. Yet, due to the opaque nature of commercial data practices, little is known about the risks or harms associated with children's data, or how it is implicated in the political economy of surveillance capitalism (Stoilova, Nandagiri, and Livingstone, 2021). Without greater understanding of what happens to personal data beyond the point of collection, arguments about children's data rights struggle to progress past arguing that the lack of transparency is itself an issue. This paper reports on the early stages of a research project that engages with this problem by examining the Australian data broker industry and its interactions with children's data. It provides analysis of the commercial and regulatory landscape of data brokering in Australia, and considers implications for both the theorisation and regulation of children's data privacy.

Data Brokers

Data brokers are companies that acquire personal data and sell it, or insights derived from it, to other entities for purposes like marketing, risk assessment, and law enforcement. Brokers occasionally collect personal data directly from individuals but more often acquire it through a combination of a) buying or trading data from private companies and government agencies and b) trawling public information such as property records, voter and motor vehicle registrations, court records, and census data. While data brokerage existed well before digital technologies, developments in behavioural data, programmatic advertising, and real time bidding have dramatically expanded the industry.

Understanding data brokers and their engagement with children's data is important in part because the industry is a characterised by a high level of 'privacy asymmetry' whereby people know little or nothing about companies that are gathering and trading their data. It is also important because of the scale and sensitivity of the data they collect. A report from the US Federal Trade Commission found that one data broker firm had 3000 data segments on nearly every US consumer (Federal Trade Commission, 2014), while in Australia, a market segmentation product from the company Quantium claims to profile 80% of Australian households (Manwaring et al., 2021). Research has indicated that some companies trade in highly-sensitive information, like mental health conditions (Kim, 2023), drug use, or sexual orientation (Manwaring et al., 2021).

While the actions of data brokers are concerning in general, their practices have specific significance for children given their unique rights (Lupton & Williamson, 2017), and the

unprecedented degree of datafication they will experience across their lifetimes (Mascheroni & Sibak, 2021). A focus on how children are implicated in data brokerage is also salient given the momentum around reforming data privacy regulations to protect children (Lomas, 2021) — a momentum which extends well beyond the appetite for regulating programmatic advertising more generally.

Mapping the Australian Industry and its Interest in Children and Families

Drawing on an analysis of company websites, media reporting, and trade publications, this paper provides a map of the current Australian data brokerage industry. It argues that the industry is characterised by a continuum of practices and business models that range from crude to highly complex and that, across this continuum, there is a clear interest in children and families as key consumer types.

At the simple end of the industry are 'list brokers' — companies that trade access to lists of contact details, like phone numbers and email addresses. Lists are categorised into consumer types, including many that focus explicitly on parents of young children, or even on children themselves. For example, one company offers a list titled 'Parents with young children' that includes contact details and demographic information about 312,000 individuals who can be targeted on the basis of their child's age. The company also offers a list called the 'National student database' which purports to contain mobile and email data for children as young as 12 years old. This company, and the many others like it, claim that they do not give clients direct access to these contact details but instead send out communication on clients behalf.

The opposing end of the industry is sophisticated multinational analytics firms that offer a wide range of products and services relating to consumer data. For these firms, the most valuable data don't exist waiting to be excavated, as is the case with phone numbers and email addresses; rather, they are created by applying analytics processes to personal data that has been aggregated from a wide range of sources. These processes generate new information, such as who is most likely to buy specific products within a specific window of time. One example is Quantium. While their privacy policy states that they do not "knowingly collect" data about anyone under the age of 13 (Quantium, 2021), it is clear from their own marketing materials that families with children are a key consumer market, and that they thus gather and process data that is about children by proxy. It is also clear that their data flows are facilitated by forms of vertical integration and 'partnerships' that extend from companies with vast amounts of consumer data, including supermarkets and banks, through to organisations that provide ad tech infrastructure, such as news media. These relationships, together with increasingly automated analytics processes, appear to avoid the need for brokers like Quantium to 'trade' data in a traditional sense.

Implications for Theory and Policy

In addition to contributing empirical insights, this work has both theoretical and regulatory implications. Scholars have become increasingly focused on conceptualising and theorising models of data privacy that resist the usual focus on individuals, including drawing attention to the need for collective rights for Indigenous data

sovereignty (Rainie et al., 2019). This paper's examination of data brokers highlights a further example where individual models of privacy are insufficient — that is, even when data brokers explicitly claim that they do not collect data about children, data that pertains to categories like 'parents' or 'new mothers' clearly includes children by proxy.

Additionally, there are both regulatory and theoretical implications that stem from a more precise understanding of brokerage practices. While scholars have argued that policy responses to data brokers need to extend beyond transparency (Crain, 2018), this work illustrates that even when regulation attempts to address practices, there are nuances to be considered. For example, in Australia where this project is focused, current proposals for privacy reform focus on tightening controls around *trading* personal data, including a proposal to "Prohibit trading in the personal information of children" (Attorney-General's Department, 2023). However, arguably neither the list brokers, nor analytics firms, focus their operations around trading personal information – – at least not in the supply of their services — raising questions about the focus on 'trading' in reform efforts and in the conceptualisation and theorisation of contemporary data brokers.

References

Attorney-General's Department (2023). *Privacy Act Review Report*. Australian Government Attorney-General's Department. https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf

Crain, M. (2018). The limits of transparency: Data brokers and commodification. *New media & society*, *20*(1), 88-104.

Federal Trade Commission (2014) *Data Brokers: A Call for Transparency and Accountability.* US Federal Trade Commission. https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

Kim, J. (2023) *Data Brokers and the Sale of Americans' Mental Health Data: The Exchange of Our Most Sensitive Data and What It Means for Personal Privacy*. Duke University Cyber Policy Program https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/02/Kim-2023-Data-Brokers-and-the-Sale-of-Americans-Mental-Health-Data.pdf

Lomas, N (September, 2021) UK now expects compliance with children's privacy design code. *TechCrunch.* https://techcrunch.com/2021/09/01/uk-now-expects-compliance-with-its-child-privacy-design-code/https://techcrunch.com/2021/09/01/uk-now-expects-compliance-with-its-child-privacy-design-code/

Lupton, D., & Williamson, B. (2017). The datafied child: The dataveillance of children and implications for their rights. *New Media & Society*, *19*(5), 780-794.

Manwaring, K., Kemp, K., & Nicholls, R. (2021). *(mis)Informed Consent in Australia*. UNSW Law Research.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3859848https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3859848

Mascheroni, G., & Siibak, A. (2021). *Datafied childhoods: Data practices and imaginaries in children's lives*. Peter Lang.

Rainie, S., Kukutai, T., Walter, M., Figueroa-Rodríguez, O. L., Walker, J., and Axelsson, P. (2019) Indigenous data sovereignty. In T. Davies, S. Walker, M. Rubinstein, F. Perini, (Eds.), *The state of open data: Histories and horizons.* African Minds and International Development Research Centre.

Stoilova, M., Nandagiri, R., & Livingstone, S. (2021). Children's understanding of personal data and privacy online–a systematic evidence mapping. *Information, Communication & Society*, *24*(4), 557-575.

Quantium (2021) *Privacy Policy.* The Quantium Group. https://quantium.com/wp-content/uploads/2022/09/Privacy-policy-27-July-2021-%E2%80%93-web-version.pdf

DATA AND PRIVACY AS A SOCIAL RELATION

Gavin Duffy
Deakin University

Introduction and Context

The EdTech market continues to grow, with a market value of 142 billion USD (Grand View Research, 2022), dozens of unicorns (Sanghvi, & Westhoff, 2022), a compound annual growth rate (CAGR) of 16.3% in the aftermath of the COVID-19 pandemic (HolonIQ, 2020). Perhaps unsurprisingly, parents are becoming increasingly concerned about their children's privacy, with the UN (Cannataci, 2021, 12) reporting that '85 per cent [of parents] have concerns about their children's digital privacy', while a survey in Australia reports parental feelings of powerlessness in combatting technological issues (Fu et al, 2019). Privacy issues are also amongst the top three concerns of young people in Australia as well, with regard to their safety online (Moody et al, 2021).

The concept of data, of course, pre-dates digital technologies. In particular, modes of schooling and education have long been predicated upon collecting, analysing, and utilising data for the purpose of stratifying students and (often) reifying existing hierarchies. This is seen across various critiques of education, whether it is Freire's (1970/2000) critique of the banking model; Bourdieu's (1974) critique of social and cultural capital through schooling, or in the use of schooling as a tool of colonialism (e.g. Welch (1988) on Australia) and white supremacy (e.g. DuBois (1973) on America) in the Global North. The function of EdTech today does not substantially differ from this stratifying aim, often replicating the same biases (Arantes, 2022), with the purported benefit of this technology being that it can do these data processes on a larger and more efficient scale than the more micro-level and more socially-constituted analogue processes of data.

Methods

Within my research, I conducted two semi-structured focus groups with primary-aged students, which included a discussion of how the students understood data and their own data practices. Focus groups were conducted in the interest of destabilising the traditional research-participant power dynamic found in interviews (Wilkinson, 1998), particularly with children (Christensen, 2004), with focus groups allowing for greater talk amongst the student participants (as well as the option of silence from individual students). Recognising and combatting these power imbalances was a conscious attempt to treat students as 'competent social actors' with their own agency, rather than as 'other' from the researcher (Cutting & Peacock, 2021, 2).

Thus, I discussed data with the student participants, asking them similar question to the adult participants in my research around EdTech and its impact on privacy. In doing so, I sought a greater understanding of how those who grow up with EdTech learn and think about their own privacy. Do so-called 'digital natives' see data in a completely different manner than older 'digital immigrants' as Prensky (2001) claimed? Indeed, some of the

teachers I interviewed appeared to believe so, suggesting that digital datafication was now simply the default for student as, simply, ‘that’s the society we live in’.

Findings Part 1

Contrarily, the conversations I had with students actually reiterated the importance of seeing data as relational and directly interpersonal, rather than a purely digital commodity. The students I spoke with initially discussed data as a type of knowledge with a social value; knowledge which can be given from one person to another but, equally, can be withheld. There are two notable elements to this. The first is that there was no technical element implied; rather, the students positioned the discussion we were having as one such exchange, in which they were ‘the knowledgeable’, while I was the one seeking new information. This initial interpretation of data as something which is not uniquely digital sits in contrast to most contemporary discussions around data and data privacy, where the digital aspect of this issue is more often than not left unsaid. The idea of ‘data’ is one which is generally now conflated with digital technologies but, evident from these students, remained ‘analogue’ as well.

Secondly, this discussion suggests that students, even at a young age, are aware (at least implicitly) of their ownership over their own data, their ability to share this data with someone else, and perhaps most importantly, their ability to withhold their data should this not consent to its collection. Data, in this case, is defined by its ability to be withheld, rather than an assumption of being shared by default. This raises a supplementary question then: do students willingly and knowingly consent to educational apps collecting their data?

Findings Part 2

It was only after I specifically reframed my questions to be about data generated through the apps the students used at school that the discussion of data became one of digital data specifically. This illuminated the second social aspect of data observed in my research: how students understand where, how, and who uses their (digital) data. The students I spoke with conceptualised their data as being used specifically by their teacher, as this is how they had seen their data being used. The students, naturally, had a pre-existing relationship with their teacher, trusted them in general, and so felt no issues with the collection, distribution, and analysis of their data through an app. In contrast, the students *did not* consider that their data would be used by a private, for-profit company, as they did not have a social connection to the app developers.

This suggests that, for younger students at least, educational technologies benefit from the goodwill cultivated by classroom teachers, taking on a meta-social capital which allows EdTech to collect student data due to the already established trust between teachers and their students. Fundamentally, this may undermine any claims towards informed consent between young students and data-harvesting apps, with the students in my research appearing to only truly give consent for their teachers to access their data.

Conclusion and Contribution

I therefore suggest a re-consideration of how we think about data in educational technologies; away from technical terms, returning to a more social conception of data. A social conception of data is one which is potentially less instrumental, less rationalised, and resultantly less easily commodified in comparison to the technical view of data, with its tendency towards a disembodied data doppelganger. Not only is this a 'social' conception of data which begins with privacy as the default status (rather than an 'option' to be tweaked), but it is one which reflects the existing, lived conception of data held by young students. In shifting towards a social idea of data then, the person (and, in this case, the student) is centred, as the originator and owner of data, who can (but is not required to) share this data with those they trust. This stands in contrast to a technical notion of data, which risks assuming data exists only once it is collected by an external, digital force, rather than being the domain of those who are surveilled by digital technologies.

Bibliography

Arantes, J. A. (2022). *The 'postdigital teacher identities' praxis: A discussion paper. Postdigital Science and Education, 4* (2), 447-466.

Bourdieu, P. (1974). The school as a conservative force: Scholastic and cultural inequalities. *Contemporary research in the sociology of education, 32* (46).

Cannataci, J. (2021). Artificial intelligence and privacy, and children's privacy. Published by: UNHRC. Available from: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/015/65/PDF/G2101565.pdf?OpenElement (accessed 24/02/2023).

Christensen, P. H. (2004). Children's participation in ethnographic research: Issues of power and representation. *Children & society, 18* (2), 165-176.

Cutting, K., & Peacock, S. (2021). Making sense of 'slippages': Re-evaluating ethics for digital research with children and young people. *Children's Geographies*, 1-13.

DuBois, W. E. B. (2001). *The education of Black people: Ten critiques, 1906-1960*. Monthly Review Press, New York.

Freire, P. (1970/2000). *Pedagogy of the Oppressed, 30th Anniversary Edition*. Continuum, New York.

Fu, E., Chesters, J., & Cuervo, H. (2019). PREPARING THE NEXT GENERATION OF AUSTRALIANS FOR UNCERTAIN FUTURES. Published by: University of Melbourne MGSE. Available from: https://education.unimelb.edu.au/__data/assets/pdf_file/0005/3027362/27818-YRC-MGSE-parenting-21st-Century-Report.pdf (accessed 24/02/2023).

Grand View Research. (2022). Education Technology Market Size, Share & Trends Analysis Report By Sector (Preschool, K-12, Higher Education), By End-user (Business, Consumer), By Type, By Deployment, By Region, And Segment Forecasts, 2023 – 2030. Available from: https://www.grandviewresearch.com/industry-analysis/education-

technology-market#:~:text=How%20big%20is%20the%20education,USD%20142.37%20billion%20in%202023 (accessed 24/02/2023).

HolonIQ. (2020). Global EdTech market to reach $404B by 2025 - 16.3% CAGR. Available from: https://www.holoniq.com/notes/global-education-technology-market-to-reach-404b-by-2025 (accessed 24/02/2023).

Moody, L., Marsden, L., Nguyen, B., & Third, A. (2021). Consultations with young people to inform the eSafety Commissioner's Engagement Strategy for Young People. Published by: Western Sydney University, Young and Resilient Research Centre. Available from: https://www.esafety.gov.au/sites/default/files/2022-01/YRRC%20Research%20Report%20eSafety%202021_web%20V06%20-%20publishing_1.pdf (accessed 24/02/2023).

Prensky, M. (2001). Digital natives, digital immigrants part 2: Do they really think differently?. *On the horizon, 9* (6), 1-6.

Sanghvi, S. & Westhoff, M. (2022). Five trends to watch in the edtech industry. Published by McKinsey & Company. Available from: https://www.mckinsey.com/industries/education/our-insights/five-trends-to-watch-in-the-edtech-industry (accessed 24/02/2023).

Welch, A. R. (1988). Aboriginal education as internal colonialism: The schooling of an Indigenous minority in Australia. *Comparative Education, 24* (2), 203-215.

Wilkinson, S. (1998). Focus groups in feminist research: Power, interaction, and the co-construction of meaning. *Women's studies international forum*, *21* (1), 111-125.

DEVELOPING A HOLISTIC FRAMWORK FOR ANALYSING PRIVACY POLICIES — A CHILD'S RIGHTS AND DATA JUSTICE PERSPECTIVE

Anna Bunn
Curtin University

Rebecca Ng
University of Wollongong

Xinyu 'Andy' Zhao
Deakin University

Gavin Duffy
Deakin University

Introduction

Contemporary childhood is frequently digital by default. Over the past years, the revolutionary expansion of technology into family homes and educational environments has transformed how and where children's play, connection and education take place. So far, much discussion and debate has been devoted to the implications of these technological solutions for children's health, connection, and education (Straker et al., 2018; Hollis et al., 2020; Undheim, 2022). We call for and contribute to a different perspective which emphasizes how this trend has significant implications for children's privacy and data rights. We point out that the growing adoption of technology across various settings, including education, has created practical challenges for researchers, educators, and families to understand how children's personal data are collected, used, and shared, as a result of their engagement with digital services.

Overwhelmingly, Australian parents believe that 'children should have the right to grow up without being profiled and targeted' and that technology in schools and for education should only 'collect the minimum personal information necessary for the service' (OAIC, 2020, 94). Young people have also advocated for more rules to limit how data of those under 18 is collected and used (Australian Government, 2022, 146). Despite this, a recent report by Human Rights Watch (HRW) identified that 89% of the education technology products they reviewed tracked children across the internet and provided children's data to third-party companies, usually in the advertising technology sector (HRW, 20220.

Typically, it is through privacy policies that those outside of the provider organisation gain insights into what personal information the provider collects and holds, how and from whom it is collected, and how it is used. However, privacy policies are often long and complex. They also frequently employ vague language that permits the provider to collect extensive amounts of personal information and use it for a wide variety of purposes, but obscures the provider's actual practices (Reidenberg et al., 2015; Australian Competition & Consumer Commission, 2019). Unsurprisingly, therefore, Australians often fail to engage with privacy policies at all or, where they do engage, fail

to understand them (OAIC, 2020, p. 69). Likewise, academics and researchers are faced with methodological challenges in unpacking the increasingly convoluted privacy policies provided by technology companies.

To address this problem, we develop new framework for analysing the privacy policies of online products and services likely to be used by children. This framework is designed to be practical and straightforward for researchers to use, while providing sufficient, relevant indicators that can be used to gain a deeper understanding of privacy policies and the extent to which they, and the data practices they indicate, reflect a child-centric approach to children's data (protecting children *within* the digital environment, not from it (Information Commissioner's Office [ICO], 2020).

Methods and Findings

We conducted a literature review on studies to identify existing frameworks for evaluating privacy policies and terms of service. This review sought to answer the following questions:

1. What are the key benefits and drawbacks of existing frameworks? This involves answering the following questions, among others: to what extent are they practical and easy to use? to what extent do they allow for a practical and holistic analysis of privacy policies? to what extent do they allow us to assess whether a privacy policy, and the practices it indicates, promotes data justice for children? to what extent are they useful in drawing comparisons between different products/services?
2. What are the primary tensions between privacy policies and the understandings of the average end-users?
3. How can privacy policies be made more relevant to end-users?
4. How can analytical frameworks for privacy policies be made more useful for researchers as well as for end-users?

Through the review, we identified four domains for evaluation: readability; visual analysis; textual and evaluative analysis; and historical analysis. In practice there is some overlap between them.

Readability considers the extent to which the privacy policy is accessible, taking into account the age and background of the intended reader or readers. Visual analysis considers the 'look and feel' of the policy and the extent to which layout, use of diagrams and so on assists to engage the reader and simplify the key messages. Textual and evaluative analysis considers how transparent the policy is (e.g. to what extent does it use vague language) and the extent to which it complies with legal requirements (specifically those contained in Australia's federal Privacy Act (the *Privacy Act 1988* (Cth). It also identifies risky practices, as well as language and terms that indicate best practice in the context of children's rights. Finally, historical analysis allows for the comparison of the current privacy policy with previous versions of the same policy, where available, to assess the extent to which practices have changed over time.

Using a set of indicators across these domains, we then developed a framework for analysing privacy policies from a child's digital rights perspective, influenced by a data justice approach. A data justice approach examines the 'fairness in the way people are made visible, represented and treated as a result of their production of digital data' (Taylor 2017, p. 1), specifically addressing groups who are traditionally marginalised in conversations around justice, and is concerned with notions of ethics, autonomy, trust, accountability, governance and citizenship (Dencik *et al.* 2019, Apps *et al.* 2022). We see young children as one such group who have thus far been under-served by the data practices of technology providers, among other organisations. From a child's rights perspective, data collection of children should be minimised and only used for the provision of a service and in the best interests of the child (ICO 2021). Adopting a child's rights perspective to information practices can therefore promote data justice for children.

The framework is intended to enable a holistic analysis of privacy policies to identify not only the extent of compliance with Australian law, but the extent to which the provider's policies, and the practices they indicate, promote a child rights approach to data and avoid 'risky' practices of most concern to parents and young people (OAIC, 2020; Australian Government, 2022). The framework can be adapted to other legal contexts and enables for the comparison of privacy practices that are indicated in the policy, with those that actually occur (so far as these are discernable).

We then tested this framework with different privacy policies and users to settle on the framework described in this paper.

Contribution

Various frameworks for analysing privacy policies exist. However, these frequently focus on one or two domains, and/or fail to provide a means to assess privacy policies holistically, and from a child-right's perspective. They often require subjective assessments to be made, which devalues their utility for comparing products. Our framework makes an important contribution by allowing for a practical, objective and holistic assessment of privacy policies that makes visible both risky practices and best practice, from a child right's perspective.

References

Andrejevic, M. (2019). Automating Surveillance. *Surveillance & Society*, *17*(1/2), 7-13. https://doi.org/10.24908/ss.v17i1/2.12930

Apps, T., Beckman, K., & Howard, S.K. (2022). Valuable data? Using walkthrough methods to understand the impact of digital reading platforms in Australian primary schools. *Learning, Media & Technology*, 1-16 https://doi.org/10.1080/17439884.2022.2160458

Australian Competition & Consumer Commission. (2019, June). *Digital Platforms Inquiry. Final Report.* https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report

Australian Government, Attorney General's Department. (2022). *Privacy Act Review*. https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf
Dencik, L., Hintz, A., Redden, J. & Treré, E. (2019). Exploring data justice: Conceptions, applications and directions. *Information, Communication & Society, 22* (7), 873-881. https://doi.org/10.1080/1369118X.2019.1606268

Hollis, C., Livingstone, S., & Sonuga-Barke, E. (2020). Editorial: The role of digital technology in children and young people's mental health – a *triple*-edged sword? *The Journal of Child Psychology and Psychiatry, 61*(8), 837-841.

Human Rights Watch. (2022, May). *How dare they peep into my private life? Children's rights violations by governments that endorsed online learning during the Covid-19 pandemic.* https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

Information Commissioner's Office. (2020). *Age appropriate design code: a code of practice for online services.* https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/

Office of the Australian Information Commissioner. (2020, September). *Australian Community Attitudes to Privacy Survey 2020.* https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey

Reidenberg, J.R., Breaux, T., Cranor, L.F., French, B., Grannis, A., Graves, J.T., Liu, F., McDonald, A., Norton, T.B., Ramanath, R., Russell, C.N. Sadeh, N., & Schaub, F. (2015). Disagreeable privacy policies: Mismatches between meaning and users' understanding. *Berkeley Technology Law Journal, 30,* 39-88.

Safer Technologies for Schools. (2022, October). *Safer Technologies for Schools Assessment: Supplier Guide.* https://st4s.edu.au/st4s-vendor-guide/

Straker, L., Zabatiero, J., Danby, S., Thorpe, K., & Edwards, S. (2018). Conflicting Guidelines on Young Children's Screen Time and Use of Digital Technology Create Policy and Practice Dilemmas. *The Journal of Pediatrics*, *202*, 300–303.

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*, *4*(2). https://doi.org/10.1177/2053951717736335

UN Committee on the Rights of the Child. (2021, March). *General comment no. 25 on children's rights in relation to the digital environment.* CRC/C/GC/25.
Undheim, M. (2022). Children and teachers engaging together with digital technology in early childhood education and care institutions: A literature review. *European Early Childhood Education Research Journal*, *30*(3), 472-489.

UNBOXING DATA AND PRIVACY VIA YOUNG CHILDREN'S WEARABLES

Tama Leaver
Curtin University

Introduction

Wearables, or wearable devices, are an increasingly common part of the adult world from FitBits to Smartwatches. In tandem, a growing market exists of wearables aimed at infants and young children. Often these devices seemingly offer important health, monitoring or educational benefits. However, signaling about what data is collected, stored, analysed and shared online by these devices is often not obvious to many consumers, including parents. Even when these wearable devices are explicitly linked to a companion app which has Terms and Conditions allowing young children's data to be harvested, these Terms and Conditions are rarely read in full, and are deliberately challenging for everyday consumers to easily navigate (Obar & Oeldorf-Hirsch, 2020). In a cultural context where dataveillance is near ubiquitous (van Dijck, 2014) and children increasingly have their data captured, collected and analysed in various ways that may create value for commercial entities (Mascheroni & Siibak, 2021; Plunkett, 2019), mapping the way children's data privacy is situated is vital.

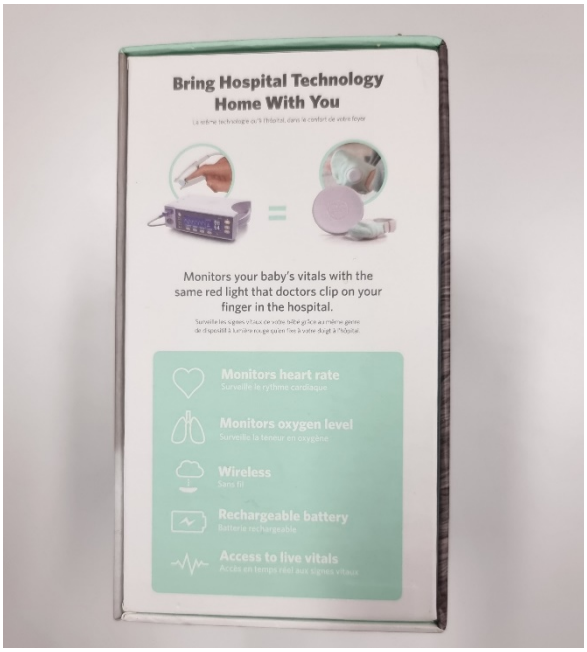
This paper explores what messages a parent or other consumer who is considering purchasing an infant wearable can evaluate prior to downloading the companion app itself. Importantly, this means a close examination of the sort of packing and boxes devices come in since these are often the first messaging about that device consumers or parents encounter. Indeed, these may be the primary messages used to decide whether or not to purchase an infant wearable. This has direct implications when the device itself connects online and often shares personal data about young children and their families and contexts. Indeed, as with many material objects, the decision to purchase a device is likely to have already been concretely made before any consideration of a companion app at all, and thus any information about the children's data is collected, and their privacy, is even further removed from a consumer/parent's consideration.

Building on existing 'walkthrough' analytical methods (Light et al., 2018), this paper offers a methodology for better 'reading' infant wearables in terms of the material signals offered by marketing materials, packaging and related promotional displays, highlighting a serious lack of signaling or transparency about how most of these devices collect, store and often own the data of very young children. The paper offers two case studies: the Owlet SmartSock2 infant wearable; and the Nurofen for Children Feversmart Temperature Monitor, and offers an unboxing methodology for other related research.

Method: Walkthrough + Unboxing

The walkthrough method developed by Light et al (2018) has become one of the most popular methodological tools within media and communications research for analysing app use. To date there have been over 500 papers using this method, but only 6 of them meaningfully focus on apps relating to physical devices and only one of those specifically examines a wearable device (Lyall, 2021). The walkthrough method is powerful as is establishes an apps' 'environment of intended use' by reading a range of signals around apps. In order to adapt this method for wearables, I borrow the forensic scrutiny of the unboxing genre of YouTube videos (Mowlabocus, 2018) to use the same analytical techniques and breadth, but with the added layer of exploring the physical packaging materials and the initial experience of removing a device and setting it up. These signals generally precede any engagement with a companion app (if there is one) and are especially important around devices aimed at parents of very young children, not least of all as these are a particular anxious and often sleep deprived group of consumers. This process then establishes *a device's environment of expected use*.

Case Study 1: The Owlet SmartSock2



Figures 1, 2, 3. Unboxing the Owlet Smart Sock 2: packaging images.

The Owlet Smart Sock is one of the most established infant wearables available today and has been particularly notable as the developers of it have been explicit in the fact that extracting, aggregating and reusing infant data is part of their business model

(Leaver, 2017). Indeed, in the US in 2021 the developers were forced to stop selling the Smart Sock for months after the FDA found their advertising deceptive (Raymond, 2021). In the US the Smartsock has been rebranded as something else, but in Australia the Smartsock is still available for purchase.

In unboxing the Smartsock 2, detailed photographs and notes were taken in first examining the packaging the device arrives in (see Figures 1, 2, 3). Marketed like a high end technology product, the packaging emphasized the ease of use, mentioned technical features, and emphasized health benefits. While there was an image pointing out there is a companion app, there was no mention of data or privacy anywhere on the outside packaging, nor inside the package where additional text appeared on the inner panels of the box. While ‘peace of mind’ is mentioned twice, the complete absence of any detail about how an infant’s data will be used, or any information about privacy, is significant in how this product is framed at the point of purchase.

Case Study 2: Nurofen for Children ‘FeverSmart’ Device

Figures 4, 5, 6. Nurofen FeverSmart Packaging, Unboxed, and Instruction Booklet Images.

The Nurofen Feversmart device retail price in Australia ranges from $99 to $139 and consists of a wearable temperature monitor that is affixed to an infant under their arm which then relays via bluetooth real-time temperature data to a paired mobile device. When unboxing the device (see Figures 4, 5, 6) there were health and medical warnings in the instruction booklet, as well as standard warnings about the included battery, but no explicit mention of data collection or children's privacy. As with the Owlet, small images refer to their being a companion app, but no further information is on the product packaging, instruction booklet, or device itself. The Nurofen web page for the product also lacks any specific information about children's data and privacy. It is not until the companion app is installed that consumers are asked for a range of private data about them and the child being monitored.

Initial Conclusions, Next Steps

In terms of children's data and privacy, as well as parents/carers ability to make informed decisions about infant data, unboxing both the Owlet Smartsock and the Nurofen Feversmart devices highlights the complete lack of information and cues for potential consumers about the way these devices generate, capture and share data about children with the commercial providers that create them. For many consumers, having made a decision to purchase a device often means they are unlikely to have the time or literacy to scrutinize unfriendly and often unreadable legal terms of use when installing a companion app. For children's current and future rights to privacy to be respected, better privacy signaling is required. At a methodological level, extending the walkthrough method with additional unboxing tools and processes expands the utility of that method which may be of use for other projects that examine wearables and devices. Next steps in this research should include developing a prototype signally or rating system for device packaging that could be mandated to better inform consumers, along the lines of star ratings about healthiness on food packaging.

References

Leaver, T. (2017). Intimate Surveillance: Normalizing Parental Monitoring and Mediation of Infants Online. *Social Media + Society*, *3*(2). https://doi.org/10.1177/2056305117707192

Light, B., Burgess, J., & Duguay, S. (2018). The walkthrough method: An approach to the study of apps. *New Media & Society*, *20*(3), 881–900. https://doi.org/10.1177/1461444816675438

Lyall, B. (2021). 'Build a future champion': Exploring a branded activity-tracking platform for children and parents. *Media International Australia*, 1329878X211007167. https://doi.org/10.1177/1329878X211007167

Mascheroni, G., & Siibak, A. (2021). *Datafied Childhoods: Data Practices and Imaginaries in Children's Lives*. Peter Lang Publishing, Incorporated.

Mowlabocus, S. (2018). ‘Let’s get this thing open’: The pleasures of unboxing videos. *European Journal of Cultural Studies*, 1367549418810098. https://doi.org/10.1177/1367549418810098

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, *23*(1), 128–147. https://doi.org/10.1080/1369118X.2018.1486870

Plunkett, L. A. (2019). *Sharenthood: Why We Should Think before We Talk about Our Kids Online*. The MIT Press.

Raymond, A. (2021, November 24). Owlet infant monitoring sock pulled following FDA warning. *Deseret News*. https://www.deseret.com/utah/2021/11/24/22801111/owlet-infant-monitoring-sock-pulled-following-fda-warning-wearable-baby-monitor-regulation

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