Selected Papers of #AoIR2019:
The 20th Annual Conference of the
Association of Internet Researchers
Brisbane, Australia / 2-5 October 2019

ENTRUSTING CHILDREN'S DATA (panel proposal)

This panel is devoted to the issue of trust and children's data. Trust in the ethical treatment of children's data relies on a broad balance of trust in a complex network of actors and practices involved in data collection, analytics, sharing and use of children's data. More specifically, trust in how data is captured, who the data is captured by, what is done to the data and how outcomes generated out of the data are employed needs to be guaranteed. We discuss the predictive practices (algorithmic analysis) used to uncover behaviours, characteristics and relationships in order to anticipate outcomes, and nudge behaviours and attitudes or initiate interventions on behalf of children. The panel also investigates how children's databases have made their way onto the dark web, positing that trust in the security of databases held by commercial and state actors is at risk. We then consider the ethical tension between the use of micro-celebrity social media influencers to establish market trust in brands and products, and the use of these potentially vulnerable influencers to market to other potentially vulnerable consumers.

Paper one 'Entrusting predictions for children's futures' discusses the future implications of large-scale data collection and analytic activities enacted across the everyday that is evident in media, academic publications and government policy discussions. Digging deeper, this concern is centred largely on unease about how the data is captured, who the data is captured by, what is done to the data and how outcomes generated out of the data are employed. Lack of transparency or clarity around internal machinic calculation processes requires 'trust' in the veracity of outputs of these systems. Children are increasingly being positioned as data sources, datafied and embedded in algorithmic ecosystems that employ a range of calculations to uncover patterns or anomalies, to highlight risk, and to predict future outcomes. These practices inform strategies, policies and planning and therefore can have material consequences that can be advantageous or disadvantageous for the child, the family and their future pathways. This presentation explores three examples of predictive practices in early childhood in the health, education and commercial sectors through an analysis of relevant academic, policy and commercial literature and discourse to highlight the raft of ways that the placing of trust in algorithmic processes needs to be carefully scaffolded and critiqued.

Suggested Citation (APA): Holloway. D., Archer, C., & Willson, M. (2019, October 2-5). *Entrusting Children's Data*. Panel presented at AoIR 2019: The 20th Annual Conference of the Association of Internet Researchers. Brisbane, Australia: AoIR. Retrieved from http://spir.aoir.org.

Paper two, ‘When trust goes wrong: Children on the dark web’ investigates what happens when trust goes wrong; when children’s personal data is hacked and circulated on the dark web? Where once child abuse material (CAM) was the only type of children’s data generally available for sale or circulation over the dark web, the growth of big data over the last decade, has seen children’s databases sourced from medical records, school records and app databases now available on the dark web—including those associated with connected toys. The paper first discusses children’s abuse material available on the dark web and then outlines the emerging availability of children’s personally identifiable information.

The paper argues that, while parents are often held accountable for their children’s digital profile and data safety, vast amounts of children’s data is being legally collected by tech companies and state actors. Some of this data has found its way onto the dark web. So far, little concern has been voiced about who is responsible for the protection of children’s data along children’s data supply chains—as well as any future ramifications of children’s data being sold and circulated on the dark web.

Paper three, ‘Trusted babes of Instagram brand-land: Child as co-opted marketer and profitable brand extension on the internet’, explores how marketers are using/exploiting consumers’ inherent love, trust and interest in children, to generate ‘brand trust’, while at the same time wading into murky ethical territory, commoditising children’s images and appeal to promote adult brands. A related phenomenon is the use of children as ‘brand extension’, where celebrity/microcelebrity influencer parents push their children as personal brand extensions, leveraging the cuteness and newsworthy impact of their own children to earn money and/or achieve fame (Archer, 2019). Far from being the ‘everyday, ordinary Internet users’ initially described in Abidin’s early definition (2015b), some child social media stars are now being presented as beyond ‘ordinary’, with lavish lifestyles or unattainable attributes presented as aspirational for the consuming public. The paper uses case studies three extreme case studies, to examine the extent to which mainstream commercial organizations/brands and parents are colluding to use still and video social media images of children (as brands in their own right) in attempt to gain consumer ‘trust’. The impact of marketers and parents co-opting children to engender this consumer ‘trust’, and the ensuing issues relevant to the digital rights of the child and the larger issue of ‘trust’ in society is also discussed.

EN/TRUSTING PREDICTIONS FOR CHILDREN’S FUTURES

Willson, Michele
Curtin University

Concern about the collection, use and possible implications of large-scale data collection and analytic activities enacted across the everyday is evident in the media, academic publications and government policy discussions. Digging deeper, this concern is centred largely on unease about how the data is captured, who the data is captured by, what is done to the data and how outcomes generated out of the data are employed. These concerns are amplified further by the opacity of the calculations and manipulations of these data sets, by proprietary restrictions and obfuscation, by the scale by which data can be gathered across the everyday and by the increasing use of

machine learning and multiple, intertwined iterative algorithmic systems. While machinic calculations are frequently positioned as neutral, objective and frequently more accurate than calculations through direct human action, numerous examples abound that demonstrate the problems with such assumptions (Bucher, 2018; Keddell, 2016; Dencik et al., 2017).

Children are increasingly being positioned as data sources, datafied and embedded in algorithmic ecosystems that employ a range of calculations to uncover patterns or anomalies, to highlight risk, and to predict future outcomes (Willson, 2019; Mascheroni, 2018; Lupton & Williamson, 2017). These systems rely heavily on various surveillance, reporting and data capture practices of the child from conception (even preconception) onwards for a range of diverse reasons and diverse stakeholders. The increasing prevalence of childhood datafication practices is attracting attention amongst privacy advocates and those working in surveillance studies, and on children's rights (Livingstone & Third, 2017; Leaver, 2015). Research that also considers the broader implications for the child in her/his every day and in terms of possible futures become increasingly important. This presentation offers this latter form of research.

Early childhood is often portrayed as the ideal time to shape, support and encourage the child in order to become fully emotionally, intellectually and socially competent adults in the future. Different theories, methods and approaches have informed these various stakeholder intentions (parent, state, commercial sector): to develop good citizens or good workers, resilient adults, and desiring consumers.
Discussions about the degree that children can participate and have agency in these shaping processes are ongoing (Livingstone & Third, 2017). However, what happens to these agentic capacities – of both adults and children – when decisions are made through data analytics and predictive algorithms drawn from variously sourced data and variable data quality? Trust in the veracity of the data collected, the accuracy of the assumptions underpinning the algorithmic calculations that have been incorporated or the (unintended) consequences that result are all questionable and should be subject to critique. We also need to consider, in Cheney-Lippold's words, 'how is this data made useful?' (2017, 46).

By predictive practices, I am referring to the use of predominantly machine learning processes using structured and unstructured data and algorithmic analysis to uncover patterns in behaviours, characteristics or relationships, to anticipate outcomes, to nudge behaviours and attitudes and to be able take pre-emptive action or acts of intervention (McQuillan, 2016). These practices inform strategies, policies and planning and therefore can have material consequences that can be advantageous or disadvantageous for the child, the family and their future pathways. For example, as Cope and Kalantzis (2016, 13) note about predictive analytics in relation to education:

> *Just as predictive analytics can be used to raise one's insurance premium or increase one's chance of arrest, so they might be used to predetermine a child's place in a learning track or a teacher's employment prospects.*

Within the contemporary child's digital ecosystem/s, there are multiple and diverse predictive practices currently and potentially at play. In the health sector, for example,

predictive machine learning algorithms are being applied to anticipate the likelihood of genetically detectable disorders in IVF pre-implantation screening (Regalado, 2017) or for the child's possibility of developing autism (Ananthaswamy, 2017); in the education sector, they are being applied to educational data to identify students at risk or those in need of particular types of targeted intervention (Smith, 2017; Clow, 2013), in the commercial sector they are being used to nudge particular types of purchasing decisions or to prompt data disclosures.

Unquestionably, human and algorithmic methods all display limitations, biases, and strengths, however, there appears to be an increasing societal reliance on machinic practices: positioning these as more objective, more efficient, more factual and therefore by default, more likely to be accurate. Lack of transparency or clarity around internal machinic calculation processes requires 'trust' in the veracity of outputs of these systems. This presentation explores three examples of predictive practices in early childhood in the health, education and commercial sectors through an analysis of relevant academic, policy and commercial literature and discourse to highlight the raft of ways that the placing of trust needs to be carefully scaffolded and critiqued.

In doing so, the paper raises questions about the broader ethical, and normative issues that become apparent for child rearing practices, data collection and the possibilities for child or parental current and future agency when predictive practices, risk aversion, and caring intent drive the choices that are made available, hidden or negated.

References

Ananthaswamy, A. (2017). Baby brain scans can predict who is likely to develop autism. *New Scientist*, 7 June. Available at https://www.newscientist.com/article/2133941-babybrain-scans-can-predict-who-is-likely-to-develop-autism/

Bucher, T. (2018). *If…Then: Algorithmic Power and Politics*. Oxford Studies in Digital Politics. New York: Oxford University Press.

Cheney-Lippold, J. (2017). *We are Data: Algorithms and the making of our digital selves*. New York: NYU Press.

Clow, D. (2013). An overview of learning analytics. *Teaching in Higher Education,* 18(6): 683-695.

Cope, B. and Kalantzis, M. (2016). Big data comes to school: implications for learning, assessment and research. *AERA Open*, 2 (2): 1– 19.

Dencik, L., Hintz, A. & Carey, Z. (2017). Prediction, pre-emption and limits to dissent: Social media and big data uses for policing protests in the United Kingdom. *New Media & Society* (online, March) 1-18, DOI: 10.1177/1461444817697722

Keddell, E. (2016). Substantiation decision-making and risk prediction in child protection systems. *Policy Quarterly*, 12(2): 46-56.

Leaver, T. (2015). Born digital? Presence, privacy, and intimate surveillance. In: Hartley, J. and Qu, W. (Eds) *Re-orientation: Translingual transcultural transmedia studies in narrative, language, identity, and knowledge*. Shanghai: Fudan University Press, pp.149-160.

Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. *New Media & Society*, 19(5), 657–670.

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

Mascheroni, G. (2018). Datafied childhoods: Contextualising datafication in everyday life. *Current Sociology,* 1-16. DOI: 10.1177/0011392118807534

Regalado, A. (2017). Eugenics 2.0: We're at the dawn of choosing embryos by health, height, and more. *MIT Tech Review*, 1 November. Available at: https://www.technologyreview.com/s/609204/eugenics-20-were-at-the-dawn-of-choosing-embryos-by-health-height-and-more/

Smith, R. (2017). The emergence of the quantified child. *Discourse: Studies in the Cultural Politics of Education,* 38(5):701-712.

Willson, M. (2019). Raising the ideal child? Algorithms, quantification and prediction. *Media, Culture & Society,* 41(5): 620-636.

WHEN TRUST GOES WRONG: CHILDREN ON THE DARK WEB

Holloway, Donell
Edith Cowan University

This paper discusses what happens when trust goes wrong; when children's personal data is hacked and circulated on the dark web? Where once child abuse material (CAM) was the only type of children's data generally available for sale or circulation over the dark web, the growth of big data over the last decade, has seen children's databases sourced from medical records, school records and app databases now available on the dark web—including those associated with connected toys. The paper first discusses children's abuse material available on the dark web and then outlines the emerging availability of children's personally identifiable information. A case study approach then traces and analyses Spiral Toys' Cloudpets 2017 data breach where children's information was hacked and placed on the dark web.

The paper argues that, while parents are often held accountable for their children's digital profile and data safety, vast amounts of children's data is being legally collected by tech companies and state actors. Some of this data has found its way onto the dark web. So far, little concern has been voiced about who is responsible for the protection of children's data along children's data supply chains—as well as any future ramifications of children's data being sold and circulated on the dark web.

Child Abuse Material

The emergence of the internet has seen greater global trade and circulation of child abuse materials. Internet technologies provide perpetrators with greater access and anonymity, and high capacity hard disks and cloud storage has made the possession of large quantities of CAM relatively unproblematic. Furthermore, the emergence of the dark web early this century has resulted in a dramatic rise in the amount, and circulation, of CAM (Drench, 2014). This is because encrypted networks, crypto-currency and block chain technology have provided the people responsible for the production, sale and circulation of child abuse materials with extra layers of anonymity (Acar, 2017).

Despite the vast scale of CAMs available on the dark web, the circulation of CAMs on the dark web provides limited financial gain for the producers and distributors of these materials. This is because piracy behaviour is widespread amongst people who download CAM; the reason being that "commercial trade of online CAMs contradict the core values of this communal group [CAM community] which has a strong tendency not to sell [but share] the abusive images they create or possess" (Acar, 2017 p. 6). As a result, new more financially profitable forms of child abuse materials are appearing. One new practice is Webcam Child Prostitution, where people pay to direct and view live-streaming video footage of minors in other countries carrying out "sexual acts in front of a webcam" (Puffer et al, 2014, slide 2). These practices involve children primarily in Southeast Asia and thousands of perpetrators from across the world. Another new practice is the crowd funding of CAM on the dark web where sellers promise to produce and provide new CAMs in exchange for crypto-currency provided by the crowd (Acar, 2017).

Children's Personal Information

Although not as immediately alarming as CAM availability on the dark web, the emerging availability of children's personal data (via big data databases) is also of concern (Van Rijmenan, 2017) Children's data chains now extends beyond corporate and state data collectors. This data is usually sourced from health records, educational records, ICT platforms, and children's apps—including those associated with connected toys.

Children's personally identifiable data (PII) is especially sought after. Their social security numbers (or other national identification numbers), birth dates, mothers' maiden names and so on are used for identity theft. This information is then used to apply falsely for welfare benefits, loans, mortgages and for tax fraud. This data is particularly valuable because children's PII provides access to clean credit histories and can go undetected for many years (Foltyn, 2018; Nettenj, 2018; Wilson, 2019).

It will take many years until these children apply for their first credit card, open loans, buy their first car, or apply for a medical health care card or welfare benefits—and will then understand that their identity, credit history and government records have been appropriated by others.

The Cloudpets™ Case

Connected toys have been implicated in the theft of children's PII and circulation on the dark web. Known data breaches include: the hacking of Mattel's Wi-Fi Hello BarbieTM (Nov, 2015), VTech's Learning LodgeTM (Nov, 2015) and CloudPetsTM (2017). CloudPets data breach, involved over 820 000 user accounts which included photos and children's names, the month and day of their birth, and 2,182,337 voice recordings. The profiles also contained the child's relationship to any adults who had been authorised to share messages with the child (Hunt, 2017).

Security expert, Troy Hunt, found that, over a six week period, many attempts were made by email, telephone, and through the company's Facebook and Twitter accounts to notify Spiral Toys of the risks to children's and customers' data. These messages went unanswered. Over this same period, parents were not informed of the breach, a requirement of the Californian government where the company is located (Hunt, 2017).

Hunt was notified of the breach by an acquaintance involved in data breach trading circles. These trading circles redistribute stolen databases either for financial gain or as a hobby. The breached databases "often spread well beyond the party that originally obtained it and the ease with which huge volumes of digital information can be replicated across the globe means that once it's exposed, it spreads rapidly" (House Committee on Energy and Commerce, 2017, p. 2).

Conclusion

Large amounts of children's data is being legally collected, analysed and shared by commercial and state actors. This same information is now being stolen and circulated on the dark web for profit. All too often, it is parents are who are held responsible for their children's digital profiles and data privacy, while at the same time some commercial and state actors are failing to maintain safe, secure databases and are vulnerable to the risk of being hacked. It needs to be recognised is that there are many players in children's data supply chains who need to be answerable for children's data privacy and security.

References

Acar, K. V. (2017). Child abuse materials as digital goods: Why we should fear new commercial forms. Retrieved from Kiel, Germany: https://www.econstor.eu/handle/10419/157247

Dredge, S. (2014, Dec 31). Study claims more than 80% of 'dark net' traffic is to child abuse sites. The Guardian. Retrieved from https://www.theguardian.com/technology/2014/dec/31/dark-web-traffic-child-abuse-sites

Foltýn, T. (2018, Jan 26). Babies' personal data hawked on dark web. welivsecurity. Retrieved from https://www.welivesecurity.com/2018/01/26/babies-personal-data-dark-web/

Hunt, T. (2017). Data from Connected CloudPets Teddy Bears Leaked and Ransomed, Exposing Kids' Voice Messages. Retrieved from https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/

Identity Verification in a Post-Breach World, House of Congress (2017).

Netten|, M. (2018, June 19). Stolen Identities of Adults, Children and Even Babies For Sale on the Dark Web. Versec. Retrieved from https://virsec.com/stolen-identities-of-adults-children-and-even-babies-for-sale-on-the-dark-web/

Puffer, E., McDonald, K., Pross, M., & Hudson, D. (2014). Webcam child sex tourism: An emerging global issue [PowerPoint slides]. Paper presented at the Research and Scholarship Symposium, Ohio. https://digitalcommons.cedarville.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1131&context=research_scholarship_symposium

Wilson, E. (2019, Feb 24). The worrying trend of children's data being sold on the dark web. TNW News. Retrieved from https://thenextweb.com/contributors/2019/02/23/children-data-sold-the-dark-web/

TRUSTED BABES OF INSTAGRAM BRAND-LAND: CHILD AS CO-OPTED MARKETER AND PROFITABLE BRAND EXTENSION ON THE INTERNET

Archer, Catherine
Murdoch University

For marketers, the issue of 'trust' is a key concern, as they strive (with business objectives in mind) to understand the psychology of consumers (Hiscock, 2001). Similarly, some marketing academics have spent their careers researching how to gain consumers' trust in brands and organisations in order to generate 'commitment' from consumers, generally for the consumers to buy (more) products and/or remain loyal customers (see, e.g., Filo, Funk, & Alexandris, 2008, Ruparelia, White & Hughes, 2010). The now seminal work of Morgan and Hunt, posited that if marketers work to develop trust through various means "such actions will enable firms and their networks to enjoy sustainable competitive advantages over their rivals and their networks in the global marketplace" (1994, p. 34). For marketers, the internet and more specifically social media, has become a relatively new field to attempt to win consumer trust in brands and generate sales (Chahal & Rani, 2017). While marketers seek the holy grail of consumer trust, they are simultaneously enlisting 'prosumer', microcelebrity social media

influencers (SMIs), who have built up social capital and 'trust' amongst their readers/viewers/followers, with large followings on their social media (Abidin, 2017; Archer, 2016).

The 'selling power' of these 'authentic' SMI storytellers has been well documented (Audrezet et al., 2018). Indeed, Influencer Marketing has become a new field of endeavour and research for marketers and marketing research (Brown & Fiorella, 2013). However, for some marketers, sociologists, consumer advocates and Government/industry regulators (to name some), the attempt by marketers to gain consumer trust through the conduit of SMIs has ironically raised ethical and trust concerns, given the SMIs often promote brands through covert means, with their Instagram, YouTube and other social media platforms filled with (often undisclosed) promotion of brands (Archer, Pettigrew & Harrigan, 2014). A related concern is the use by marketers of potentially vulnerable (liminal) influencers to market to other potentially vulnerable consumers, for example mothers (Archer & Harrigan, 2016).
A more recent development has been the use of children as social media influencers, or micro-microcelebrities (Abidin, 2015a), co-opted (through their parents as agents) to push products. While the use of children to market goods and services has been a popular technique with a long history, SMI children are now a growing phenomenon. This paper explores how marketers are using/exploiting consumers' inherent love, trust and interest in children, to generate 'brand trust', while at the same time wading into murky ethical territory, commoditising children's images and appeal to promote adult brands. A related phenomenon is the use of children as 'brand extension', where celebrity/microcelebrity influencer parents push their children as personal brand extensions, leveraging the cuteness and newsworthy impact of their own children to earn money and/or achieve fame (Archer, 2019). Far from being the 'everyday, ordinary Internet users' initially described in Abidin's early definition (2015b), some child social media stars are now being presented as beyond 'ordinary', with lavish lifestyles or unattainable attributes presented as aspirational for the consuming public.

The paper details through three extreme case studies, the extent to which mainstream commercial organizations/brands and parents are colluding to use still and video social media images of children (as brands in their own right) in attempt to gain consumer 'trust'. Publicly available Instagram posts, promotional material and mainstream media articles are explored for three social media micro-microcelebrities from Australia, the Philippines and Japan. These Instagram and brand sensations include Baby Chanco in Japan, who has been 'adopted' by shampoo giant Pantene as the 'face'/hair model of their shampoo (ABC Radio, 2019), and Scarlet Snow Belo, the Filipina three-year-old daughter of plastic surgeon/cosmetics brand owner parents, who is used to promote her parents' business interests (Aguiler, 2018). Further the paper explores the impact of marketers and parents co-opting children to engender consumer trust in brand and the ensuing issues relevant to the digital rights of the child and the large issue of 'trust' in society. I argue that focusing on children as brand and influencers of 'trust' is important because, as Livingstone & Third (p 662) posit: "the child – as a cypher for our cultural anxieties and a focus of investment for our future desires – represents an important figure through which to (re)think the digital and human rights, one in which there is almost too much at stake."

References

ABC Radio (2019) Inside the lucrative child modeling business behind Instagram phenom Baby Chanco Retrieved from: https://wtop.com/social-media/2019/02/inside-the-lucrative-child-modeling-business-behind-instagram-phenom-baby-chanco/

Abidin, C. (2015a) "Micromicrocelebrity: Branding Babies on the Internet." *M/C Journal* 18 (5):1-6

Abidin, C. (2015b) Communicative intimacies: Influencers and perceived interconnectedness. *Ada: A Journal of Gender, New Media, and Technology*, (8).

Abidin, C. (2017). Influencer extravaganza: Commercial “lifestyle” microcelebrities in Singapore. In L. Hjorth, H. Horst, A.Galloway, G. Bell *(*Eds). *The Routledge Companion to Digital Ethnography* (pp. 184-194). Routledge.

Aguilar, K. (2018). Scarlet Snow is ‘The Future of Beauty’ in digital magazine cover. Retrieved from: https://entertainment.inquirer.net/300831/scarlet-snow-is-the-future-of-beauty-in-digital-magazine-cover#ixzz5giAUghVl

Archer, C. (2019) Pre-schooler as brand extension: a tale of Pixie’s bows and birthdays. In: Green L, Holloway DJ, Stevenson KJ, et al. (Eds) Digitising Early Childhood. Newcastle: Cambridge Scholars Publishing,
pp. 58–73.

Archer C & Harrigan P (2016) Prosumers with passion: learning what motivates bloggers as digital influencer stakeholders. *PRism* 13(1), 1–14.

Archer, C., Pettigrew, S., & Harrigan, P., (2014), A Tale of Power, Passion and Persuasion: Bloggers, Public Relations and Ethics, *Asia Pacific Public Relations Journal,* 15(1), 37-54.

Ashley, C., & Tuten, T. (2015). Creative strategies in social media marketing: An exploratory study of branded social content and consumer engagement*. Psychology & Marketing,* 32(1), 15-27.

Audrezet, A., De Kerviler, G. & Moulard, J.G., 2018. Authenticity under threat: When social media influencers need to go beyond self-presentation. *Journal of Business Research*.

Brown, D., & Fiorella, S. (2008*). Influence Marketing How to Create, Manage, and Measure Brand Influencers in Social Media Marketing*. Routledge.

Chahal, H., & Rani, A. (2017). How trust moderates social media engagement and brand equity. *Journal of Research in Interactive Marketing*, 11(3), 312-335.

Filo, K., Funk, D. C., & Alexandris, K. (2008). Exploring the role of brand trust in the relationship between brand associations and brand loyalty in sport and fitness. *International Journal of Sport Management and Marketing*, *3*(1-2), 39-57.

Hiscock, J. (2001), “Most trusted brands”, *Marketing*, March, pp. 32-3

Livingstone, S., & Third, A. (2017). Children and young people’s rights in the digital age: An emerging agenda. *New Media and Society*, 19(5), 657–670

Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *Journal of Marketing,* 58(3), 20-38.

Ruparelia, N., White, L., & Hughes, K. (2010). Drivers of brand trust in internet retailing. *Journal of Product & Brand Management*, 19(4), 250-260.