Centre for Excellence in Child and Family Welfare

Draft Children's Online Privacy Code

Introduction

About the Centre

The Centre for Excellence in Child and Family Welfare (the Centre) is the peak body for child and family services in Victoria and Tasmania, representing over 150 member organisations that deliver early intervention, family support, out-of-home care, disability and allied health services across the state. The Centre's mission is to advocate for policies, programs and systems that promote the safety and wellbeing of children and young people, and that support families to thrive.

The Centre welcomes the Exposure Draft of the Privacy (Children's Online Privacy) Code 2026 and the child-centred approach which has been taken. The decision to centre the best interests of the child as the governing principle of the Code is a significant step in Australian privacy obligations.

Scope of this submission

Children's privacy is fundamental to their dignity, autonomy, and participation in civic and social life (United Nations Committee on the Rights of the Child [UNCRC Committee], 2021). As children's ability to learn, play, seek help and form relationships becomes increasingly reliant on digital devices, the question of who controls children's information (and to what ends) has become profoundly important. Data about children is currently being collected on an unprecedented scale, often without transparency, and used in ways that children and their families cannot always understand, anticipate or challenge (Lupton & Williamson, 2017; Third et al., 2019).

The Centre's members provide a wide range of services to children and families whose lives are captured in multiple databases and systems. Children engaged with child protection and family services are often subjected to data collection across multiple government agencies, courts, non-government service providers, and digital platforms throughout their childhoods. For many, the information held about them (records of abuse, neglect, mental health, and trauma) is amongst the most sensitive that any institution could hold (Eubanks, 2018; Gillingham, 2019) and yet is not visible to them or owned by them. These children deserve the strongest protections that the Code can afford.

Children's safety, identity, and future opportunities are placed at risk when their information is shared without adequate safeguards (Saxena et al., 2021; van der Kolk, 2014). Given these risks, our submission addresses the following priority themes:

- The need for explicit protections for children in child protection, out-of-home care, and family services contexts.
- Operationalising the 'best interests of the child' standard with reference to established child welfare and rights frameworks.

- Consent provisions and their interaction with children who lack safe or appropriate parental responsibility and oversight.
- The equity and safety implications of age assurance mechanisms.
- Privacy impact assessment requirements.
- Transparency obligations and age-appropriate design for children with complex needs.

The Code is an opportunity to affirm that every child, regardless of their circumstances, has a right to privacy which must be actively upheld, not merely theoretically available (United Nations, 1989, Art. 16).

The children who are most at risk are those who do not have a ‘person with parental responsibility’ in any practical sense (including those under state guardianship where parental authority is vested in a government Minister (AIHW, 2023)); children whose parents or carers pose a risk to their safety (Campo, 2015; Humphreys & Healey, 2017); children who have experienced multiple placement changes and whose digital footprints become fragmented (Mendes & Rogers, 2020); children whose cognitive or developmental disabilities and/or trauma limits their capacity to engage with privacy processes (Hill et al., 2016; United Nations, 2006); and Aboriginal and Torres Strait Islander children, whose privacy interests have a cultural and collective dimension not fully captured by the Code (Kukutai & Taylor, 2016; Productivity Commission, 2020).

The Centre urges the OAIC to make sure the final Code closes the gap between the privacy rights that law confers on and the privacy protections children in vulnerable circumstances experience.

Definitions and scope

Definition of ‘person with parental responsibility’

While it is pleasing to see that the Code’s definition of ‘person with parental responsibility’ extends beyond a biological parent, it does not capture the nuances and complexities of caregiving roles. More clarity is needed in relation to caring in child protection contexts. Here, the legal framework of parental responsibility is more complex than a binary definition can capture.

In Australia, approximately 47,000 children were in out-of-home care on any given night in 2021-22 (AIHW, 2023). For a substantial proportion, parental responsibility (in whole or in part) is vested in a state or territory Minister, chief executive or equivalent statutory officer. When a digital platform requires parental consent before collecting a child’s personal information, and the legal ‘parent’ is a government minister, there is no clear mechanism by which that consent can be obtained or communicated. The foster or kinship carer who knows the child and is best placed to make genuine judgments on their behalf has no legal standing under the Code’s current framework (Mendes, 2021; Muir et al., 2019) and the definition does not include shared parental responsibility or informal kinship care arrangements, which are common configurations in child protection practice across Australia.

Definition of ‘age appropriate’

The Code’s benchmark of tailoring communications to a child aged 10 to 12 years is grounded in developmental psychology (Crone & Konijn, 2018). However, for the children most likely to interact with child and family services, chronological age is insufficient to indicate communicative capacity.

Many children who come into contact with child protection services have experienced significant adverse childhood experiences (such as abuse, neglect, domestic violence, and parental substance use) which are associated with disrupted neurodevelopment and reduced capacity to process complex information or engage with abstract concepts such as consent and privacy (Felitti et al., 1998; Shonkoff et al., 2012; van der Kolk, 2014). The UNCRC Committee’s General Comment No. 12 (UNCRC Committee, 2009) explicitly recognises that children’s capacity to participate meaningfully in decisions about their own lives is largely dependent on how adults and institutions support this participation.

Scope: Government operated systems

The Centre supports the Code's extension to services 'primarily concerned with the activities of children'. However, many of the digital platforms which collect large amounts of sensitive personal information about children in child protection contexts are not commercial consumer services but government-operated or government-contracted case management systems. These systems hold extraordinarily sensitive information about children, often from birth through to adulthood without the children's consent or knowledge (Gillingham, 2019; Saxena et al., 2021). It is not clear from the Codes's current framing whether these systems fall within its scope, and the Centre submits that the OAIC should take a clear position on this.

Core obligations: Age assurance, data minimisation, and best interests

Age assurance

The Centre supports the Code's risk-proportionate, technology-neutral approach to age assurance. It recognises the diversity of services in scope and avoids mandating specific methods that could quickly become outdated or that carry their own privacy costs. However, for many children in child protection and out-of-home care contexts, common age assurance mechanisms are not practically accessible.

Parental verification assumes the availability of a parent who knows the child and who will positively support their digital participation. For children in residential care, children whose contact with parents is restricted by court order, or children in informal kinship arrangements, this assumption is problematic (Barnardo's, 2019). AI-based age estimation tools present additional concerns as research has documented significant accuracy disparities across demographic variables (e.g., skin tone and socioeconomic background) (Buolamwini & Gebru, 2018; Raji & Buolamwini, 2019). This raises real concerns about whether these tools will disadvantage Aboriginal and Torres Strait Islander children, and children from migrant backgrounds.

Additionally, for children whose physically safety depends on the confidentiality of their identity and location, age assurance tools that collect biometric data could unintentionally compromise a child's safety (Gillingham, 2019). The Code's requirements to destroy sensitive age-verification data 'as soon as practicable' is an important safeguard but not defined and needs to be strengthened.

Data minimisation: strictly necessary information

The Centre strongly endorses the requirement that service providers only collect, use and disclose information which is strictly necessary to enable effective service delivery.

This principle is critically important in the context of child and family services. Education technology platforms, therapeutic applications, family communication tools, and social media services used by children and young people routinely collect more data than is necessary for their stated purpose (Livingstone et al., 2019; Mascheroni & Holloway, 2019). For children who have no capacity to negotiate the terms of their data relationship with a platform, this overcollection creates risks that extend into the future (Ausloos, 2020). The 'strictly necessary' standard will require careful interpretive guidance to be applied consistently; what is strictly necessary for a case management system is different from what is strictly necessary for a gaming platform or a therapeutic chatbot.

Best Interests of the Child

The Centre considers the requirement that any collection, use, or disclosure of a child's personal information be consistent with their best interests to be the most important substantive provision in the Code. Its inclusion brings Australian privacy law into meaningful alignment with Article 3 the UNCRC (United Nations, 1989), which requires the best interests of the child to be a primary consideration in all actions concerning children.

'Best interests' is not a self-executing standard. As the UNCRC Committee's General Comment No. 14 makes clear (UNCRC Committee, 2013), a genuine best interests assessment requires active individualised consideration of a range of factors including the child's own views, developmental stage, care and protection needs, family environment, health, and particular vulnerability. The Code's explanatory materials and guidance must give entities concrete direction on what a best interests assessment in the data privacy context looks like.

Three specific applications of this principle concern the Centre particularly. First the use of profiling and algorithmic decision-making. Predictive risk assessment tools used in child welfare are increasingly deployed despite growing evidence of their tendency to encode and amplify historical biases against marginalised groups, their limited predictive validity, and their opacity to both practitioner and families (Chouldechova et al., 2018; Eubanks, 2018; Keddell, 2019). A best interests framework that does not explicitly address these risks is inadequate to the current technological landscape. Second, direct marketing targeting vulnerability. The deployment of commercial persuasion techniques against children whose online behaviour reflects their distress in out-of-home care or engaging with mental health services should not be served targeted advertising derived from that fact. Third, and most fundamentally, the Code must make unambiguous that where the best interests of the child and the commercial interests of an entity are in tensions, the child's interests must prevail (United Nations, 1989, Art. 3).

Consent

Children in Child Protection Contexts

The Code's consent framework sets 15 years at the threshold for independent consent and requires parental consent for children below that threshold. The Centre supports the rigour of these protections. However, their application in the child protection context creates significant structural problems that the Code does not currently address.

The consent model is premised on the existence of a 'person with parental responsibility' who is accessible to the entity seeking consent, empowered to give that consent, and acting in the child' best interests. For the tens of thousands of Australian children in out-of-home care at any given time (AIHW, 2023), this premise does not hold. The foster or kinship carer who knows the child and can exercise genuine judgement on their behalf frequently lacks the legal authority to do so (Mendes, 2021). The result is that the consent framework, intended to protect children in care, may in practice prevent them from accessing services their peers use routinely, a form of digital exclusion with real consequences for development, social connection, and wellbeing.

The self-consent exception for a child seeking legal or health information in connection with a person with parental responsibility provides important but insufficient relief. Children in the child protection system frequently need to access online support in relation to their own situation within the system (e.g., their placement, their legal rights, their complaints options, their safety, and their access to independent advocacy) (Parkinson, 2019). The current drafting does not clearly cover these circumstances. The right of children to participate in decisions about their own lives is explicitly protected under Article 12 of the UNCRC (United Nations, 1989) and must be given meaningful operational effect, particularly for children whose circumstances mean that adult advocacy is unreliable or unavailable.

Dark Patterns and Manipulative Design

The prohibition on seeking consent through coercive or manipulative practices is strongly support by the Centre. The digital environment children inhabit are saturated with 'dark patterns', which include design practices expressly engineered to compromise autonomous choice through pre-selected consent options, friction-laden opt-out processes, artificial urgency notifications, and interfaces that present consent as a condition of full-service access (Luguri & Strahilevitz, 2021; Nairn & Fine, 2008).

Children are developmentally less equipped than adults to recognise and resist these techniques. Their capacity for long-term consequential thinking is still developing, and their experience of digital environments as social spaces makes the social costs of opting out feel disproportionately high (Crone & Konijn, 2018). For children in care whose sense of social connection is already fragile, these pressures are intensified. The prohibition on manipulative consent practices is therefore not merely a technical compliance requirement, but also a substantive child protection measure. The current drafting does not detail specific prohibited practices, leaving interpretation to guidance. As such, the Centre urges that concrete specification are added as an essential detail.

Transparency

Child-Directed Privacy Policies

The requirement to maintain a version of privacy policies directed at children is a significant step toward making privacy information genuinely accessible rather than nominally available. Research notes that current privacy policies (including those purportedly designed for young users) fail to comprehensively communication meaningful information to children, relying on legalistic vocabulary and technical framing that adults without specialist knowledge also struggle to understand (Cranor, 2012; Luger et al., 2013).

For children in child and family services, child-directed privacy policies must go beyond explaining data collection practices in general terms. The principle of transparency requires that information flow in a direction the recipient can understand (Floridi et al., 2018; Solove, 2021). Children engaging with child and family services need to understand specifically; what information the service holds about them, who else might receive it (including government agencies and courts), what they can do if they want to access, correct or delete their information, and who they can contact if they are concerned. The Centre also notes that the co-design of child-directed privacy policies with children, particularly those with lived experience, is both the right approach and likely the most effective one (Third et al., 2019).

Automated Decision-Making Disclosure

The provision that a child or person with parental responsibility may request information about any automated decision-making relating to a child's personal information is welcome, but significantly under-powered relative to the scale of the problem it seeks to address.

Algorithmic and predictive analytics tools are now deeply embedded in child welfare practice in Australia. Structured decision-making tools and predictive risk assessment models are used across child protection intake, investigation, and placement decisions in multiple jurisdictions. These tools can shape decisions that alter the course of a child's life. Research has documented serious concerns regarding how these tools embed historical biases against Aboriginal and Torres Strait Islander families and families experiencing poverty, and they provide no meaningful avenue for challenge by the families they affect (Chouldechova et al., 2018; Eubanks, 2018; Gillingham, 2019; Keddell, 2019; Saxena et al., 2021). Making information about these tools available only upon request is insufficient. Children and families are frequently unaware that algorithmic tools have been used in decisions about them and therefore do not know to make a request.

Erasure, Monitoring, and Privacy Impact Assessments

Right to Erasure

The right for a child or their representative to request the destruction of specified information in strongly support by the Centre. The ability to limit one's permanent digital record is a fundamental condition of genuine privacy, and it is particularly important for children whose information is collected from the earliest stages of life, retained indefinitely, and use in way they cannot anticipate (Ausloos, 2020).

For children in the child protection system, the stakes are especially high. Records of abuse, neglect, mental health, and involvement with child protection services have the potential to affect children's employment, relationships, and social standing well into adulthood if retained beyond the period of legitimate use. The Centre recognised that the exceptions to destruction (including information required to be retained by Australian law and information relevant to existing or anticipated legal proceedings) are appropriate and necessary. However, a refusal notice citing statutory retention obligations in legalistic terms is not meaningfully accessible to a child (Pleasant et al., 2016; van der Kolk, 2014) who wanted to know why the platform would not delete their account.

Monitoring and geolocation

The requirement that entities providing monitoring or geolocation mechanisms notify the child of the existence and use of those mechanisms in an age-appropriate way is strongly supported. The right to know that one is being watched or tracked is a basic condition of personal dignity and a necessary prerequisite to meaningful autonomy.

The provision is particularly significant in the out-of-home care context, where monitoring of children's digital activity, physical location, and social connections is a common feature of placement managements (sometimes for legitimate safety reasons, and sometimes in ways that go beyond what is proportionate or necessary). Research on children's experiences in residential and foster care consistently shows that intrusive monitoring is one of the most common sources of grievance among children in care, contributing to feelings of powerlessness and distrust in carers (Barnardo's, 2019; Lyon, 2018; Lyon, 2018). The UNCRC is explicit that children in care retain their right to privacy, including protection from arbitrary interference with their private life (United Nations, 1989, Arts. 16, 37). The Centre notes that the notification obligation in the Code applies to entities providing the monitoring services, not necessarily the carers or services that deploy it, raising questions about whether it effectively reaches children in situations where the tool is controlled by their carer or care organisations.

Mandatory Privacy Impact Assessments

The Centre strongly supports mandatory Privacy Impact Assessments (PIAs) before introducing new services or significantly changing how children's personal information is handled, and to maintain and publish a register of these assessments. The principle of privacy by design (building privacy protection into systems from the ground up) is well-established as the most effective approach to preventing privacy harms (Cavoukian, 2011; Wright & De Hert, 2012).

The importance of rigorous PIAs is especially critical in the child and family services context, where new digital tools are continually evolving, often without adequate assessment of their privacy implications. Research examining the introduction of data-driven technologies in child welfare has repeatedly documented a pattern of implementation outpacing governance, and that tools are deployed before their bias properties are understood, before data retention practices are reviewed, and before the children and families affected have any opportunity to understand or contest their use (Eubanks, 2018; Gillingham, 2019; Saxena et al., 2021). The requirement that PIA registers be published online is a significant transparency measure (Floridi et al., 2018), but a register of titles and dates is of limited value without meaningful summaries of findings being publicly available.

Privacy education and training

The requirement for annual training of all staff and contractors with regular or frequent access to children's personal information is strongly supported by the Centre. The child and family services workforce operate under significant complexity, managing sensitive information across multiple digital environments, often under time pressure, with high caseloads, and frequent staff turnover. The conditions for inadvertent privacy breaches are structurally embedded in the way this sector operates, and purposeful, ongoing training is an essential countermeasure (Parsons et al., 2017; Solove, 2021).

However, the effectiveness of training in this context depends critically on its relevance. Generic privacy compliance training will not adequately equip a child protection caseworker, a residential care support worker, or a therapeutic program practitioner to navigate the specific privacy challenges that they encounter. Training for this workforce must address the intersection of privacy obligations, child protection mandatory reporting requirements, court order restrictions, information sharing protocols, and the ethical dimensions of digital use with children in vulnerable circumstances (van der Kolk, 2014).

Recommendations

1. **Definition of 'person with parental responsibility':** The Centre recommends that the OAIC provide supplementary guidance, with examples, of how the definition applies in child protection contexts (including state guardianship, delegated authority arrangements, shared parental responsibility, and kinship and foster care). The Code's explanatory materials should also explicitly acknowledge that, for children under guardianship orders, the relevant 'person with parental responsibility' for consent purposes is the legal guardian (including government entities), with practical guidance on how consent can be obtained in such circumstances.
2. **Definition of 'age appropriate':** Explanatory guidance should clarify that, wherever possible, 'age appropriate' communication takes into account the child's developmental capacity and not chronological age alone, particularly for services likely to be accessed by children with disability, trauma backgrounds, or complex needs. Entities should be encouraged to develop user-friendly, accessible privacy communications.
3. **Scope and government-operated platforms:** The OAIC needs to provide guidance on whether government-operated digital platforms which handle children's personal information in the context of child protection and family services (including case management and court information systems, and risk assessment tools) fall within the Code's scope. Where such systems are excluded from the Code's direct application, the OAIC should make a formal recommendation to relevant Commonwealth, state, and territory agencies that equivalent best interests, data minimisation, transparency, and destruction standards be adopted through administrative policy or legislative amendment.
4. **Age assurance:** The Code or its guidance should address how entities handle age assurance where a child does not have a parent or carer with the legal authority or practical capacity to verify. What alternative verification pathways could be accessible to children in care? The Centre also recommends that guidance be provided specifying a maximum timeframe within which entities must destroy sensitive information collected for age assurance purposes.
5. **Data minimisation and strictly necessary information:** The OAIC should provide sector-specific guidance for services targeting children in health, education, social services, and family support on how to apply the 'strictly necessary' standard in practice. This should include a framework for assessing which data categories are necessary for specific service functions. The OAIC should specify that behavioural tracking, profiling, and engagement analytics which go beyond what is operationally required are not 'strictly necessary' and should require explicit justification before being applied to child users.
6. **Best interests of the child:** The Code should explicitly state that in assessing whether data handling is consistent with a child's best interests, entities must have primary regard to the child's safety, wellbeing, and developmental needs, consistent with the UNCRC (United Nations, 1989) and General Comment No. 14 (UNCRC Committee, 2013). OAIC guidance needs to address profiling, targeted advertising, automated decision-making, and third-party data sharing.
7. **Consent for children in child protection and state care:** The Code needs to address the mechanics of consent for children in state guardianship or under child protection orders, producing guidance in

consultation with state and territory child protection authorities, care leaver advocacy organisations, and children with lived experience of care.

8. **Coercion, manipulation, and dark patterns:** The OAIC should publish a list of prohibited design practices in the context of children's consent, drawing on the European Data Protection Board's Guidelines on Dark Patterns (European Data Protection Board, 2022) and the ICO's Age-Appropriate Design Code (ICO, 2021). This list should specifically address design practices common in social media platforms, gaming environments, and health and wellbeing applications frequently used by children and young people engaged with family services. The OAIC should establish a mechanism for ongoing identification and prohibition of emerging dark patterns as digital design practices evolve.
9. **Child-directed privacy policies:** Child-directed privacy policies should be required to specifically explain, in age-appropriate terms, the circumstances in which the service may share a child's information with government agencies, courts, law enforcement, or other third parties, and the rights the child has in those circumstances. The Centre recommends the OAIC mandate or strongly incentivise the co-design of child-directed privacy policies with children, including those with lived experience of the child protection system, consistent with Article 12 of the UNCRC (United Nations, 1989) and participatory design principles (Third et al., 2019).
10. **Automated decision-making disclosure:** The Code should require entities to proactively notify children and persons with parental responsibility in plain, age-appropriate language when automated or algorithmic tools have contributed to any decision that materially affects the child. The Centre calls on the OAIC to engage with state and territory child protection authorities on the implications of this provision for predictive risk assessment tools used in child protection intake and investigation.
11. **Right to erasure and destruction of personal information:** Where entities refuse to destroy a child's personal information under a statutory exception, the notice provided to the child must be genuinely child-appropriate; explaining in plain language what is being retained, which exception applies, why that exception is relevant to the child's particular situation, and how long the information will be kept. The Centre recommends the Code specify a reasonable maximum retention period once the purpose for which information was collected has been fulfilled.
12. **Monitoring and geolocation:** The OAIC needs to explicitly confirm that services providing geolocation tools used in out-of-home care, residential care, or family support contexts are bound by the Code's notification requirements. The child's right to be informed about monitoring cannot be waived by a carer, care organisation or service provider. The Centre recommends the OAIC consult with care leaver advocates, residential care providers, and peak bodies representing children in care in developing this guidance.
13. **Privacy Impact Assessments:** The OAIC should develop a PIA template specifically tailored to services engaging children in child protection, out-of-home care, or family support contexts. There are specific risks associated with these cohorts (including risks of algorithmic bias, data breaches affecting children's safety, and long-term retention of sensitive childhood records). The Code or supporting guidance should specify that PIA registers include meaningful summaries of the findings and recommendations of each assessment so that affected individuals and communities can engage substantively with the outcomes.
14. **Privacy education and training:** Privacy education and training for staff working with children in child protection, out-of-home care, and family services must specifically address the intersecting privacy challenges of child welfare practice (including mandatory reporting, information sharing, court orders, digital safety, and the ethics of data use with vulnerable children) rather than generic privacy compliance content. Training should be developed using evidence-based approaches to professional learning in high-stakes environments (Parsons et al., 2017), including scenario-based learning, reflective practice, and regular refreshment to address emerging digital risks.

References

Australian Institute of Health and Welfare. (2023). *Child protection Australia 2021–22* (Child welfare series no. 77, Cat. no. CWS 87). AIHW.

Ausloos, J. (2020). *The right to erasure in EU data protection law: From individual rights to effective protection*. Oxford University Press.

Barnardo's. (2019). Who's looking out for them? Barnardo's.

Bijleveld, G., Dedding, C., & Bunders-Aelen, J. (2015). Children's and young people's participation within child welfare and child protection services: A state-of-the-art review. *Child & Family Social Work*, 20(2), 129–138. https://doi.org/10.1111/cfs.12082

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, 81, 1–15.

Campo, M. (2015). *Children's exposure to domestic and family violence: Key issues and responses* (CFCA Paper No. 36). Australian Institute of Family Studies.

Cavoukian, A. (2011). *Privacy by design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario.

Chouldechova, A., Benavides-Prado, D., Fialko, O., & Vaithianathan, R. (2018). A case study of algorithm-assisted decision making in child maltreatment hotline screening decisions. *Proceedings of Machine Learning Research*, 81, 1–15.

Cranor, L. F. (2012). Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *Journal on Telecommunications and High Technology Law*, 10(2), 273–308.

Crone, E. A., & Konijn, E. A. (2018). Media use and brain development during adolescence. *Nature Communications*, 9(1), Article 588. https://doi.org/10.1038/s41467-018-03126-x

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.

European Data Protection Board. (2022). *Guidelines 3/2022 on dark patterns in social media platform interfaces: How to recognise and avoid them* (Version 2.0). EDPB.

Felitti, V., Anda, R., Nordenberg, D., Williamson, D., Spitz, A., Edwards, V., Koss, M., & Marks, J. (1998). Relationship of childhood abuse and household dysfunction to many of the leading causes of death in adults. *American Journal of Preventive Medicine*, 14(4), 245–258. https://doi.org/10.1016/S0749-3797(98)00017-8

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People — An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, 28(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5

Gillingham, P. (2019 The Development of Algorithmically Based Decision-Making Systems in Children's Protective Services: Is Administrative Data Good Enough?. *British Journal of Social Work*, 50(2), 565-580. https://doi.org/10.1093/bjsw/bcz157

Humphreys, C., & Healey, L. (2017). *Research and practice insights: Children's contact with domestic violence perpetrators*. Australian Centre for the Study of Sexual Assault.

Information Commissioner's Office. (2021). *Age appropriate design: A code of practice for online services*. ICO. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/

Keddell, E. (2019). Algorithmic justice in child protection: Statistical fairness, social justice and the implications for practice. *Social Sciences*, 8(10), 281. https://doi.org/10.3390/socsci8100281

Kukutai, T., & Taylor, J. (Eds.). (2016). *Indigenous data sovereignty: Toward an agenda*. Australian National University Press. https://doi.org/10.22459/CAEPR38.11.2016

Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). *Children's data and privacy online: Growing up in a digital age. An evidence review*. London School of Economics and Political Science.

Luger, E., Moran, S., & Rodden, T. (2013). Consent for all: Revealing the hidden complexity of terms and conditions. *In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2687–2696). ACM. https://doi.org/10.1145/2470654.2481371

Luguri, J., & Strahilevitz, L. J. (2021). Shining a light on dark patterns. *Journal of Legal Analysis*, 13(1), 43–109. https://doi.org/10.1093/jla/laaa006

Lupton, D., & Williamson, B. (2017). The datafied child: The dataveillance of children and implications for their rights. *New Media & Society*, 19(5), 780–794. https://doi.org/10.1177/1461444816686328

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity Press.

Mascheroni, G., & Holloway, D. (Eds.). (2019). *The Internet of Toys: Practices, affordances and the political economy of children's smart play*. Palgrave Macmillan.

Mendes, P. (2021). Ending Australia's status as a leaving care laggard: The case for a national extended care framework to lift the outcomes for young people transitioning from out-of-home care. *Australian Social Work*, 75(1), 122–132. https://doi.org/10.1080/0312407X.2021.1910323

Mendes, P., & Rogers, J. (2020). Young people transitioning from out-of-home care: What are the lessons from extended care programmes in the USA and England for Australia?. *The British Journal of Social Work*, 50(5), 1513–1530. https://doi.org/10.1093/bjsw/bcaa028

Muir, S., Purtell, J., Hand, K., & Carroll, M. (2019). *Beyond 18: The longitudinal study on leaving care. Wave 3 research report: Outcomes for young people leaving care in Victoria*. Australian Institute of Family Studies.

Nairn, A., & Fine, C. (2008). *Who's messing with my mind? The implications of dual-process models for the ethics of advertising to children. International Journal of Advertising*, 27(3), 447–470.

Parkinson, P. (2019). *Child protection law and the family law system*. Thomson Reuters.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, 66, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

Pleasant, A., Rudd, R., O'Leary, C., Paasche-Orlow, M., Allen, M., Alvarado-Little, W., Myers, L., Parson, K., & Rosen, S. (2016). Considerations for a new definition of health literacy. Discussion Paper. *National Academy of Medicine*.

Productivity Commission. (2020). *Indigenous child protection (Research paper)*. Productivity Commission.

Raji, I., & Buolamwini, J. (2019). Actionable auditing: Investigating the impact of publicly naming biased performance results of commercial AI products. *In Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 429–435). ACM. https://doi.org/10.1145/3306618.3314244

Saxena, D., Badillo-Urquiola, K., Wisniewski, P., & Guha, S. (2021). A framework of high-stakes algorithmic decision-making for the public sector developed through a case study of child-welfare. Proceedings of the ACM on Human-Computer Interaction, 5(CSCW2), Article 348. https://doi.org/10.1145/3476089

Shonkoff, J., Garner, A., Committee on Psychosocial Aspects of Child and Family Health, Committee on Early Childhood Adoption and Dependent Care, & Section on Developmental and Behavioral Pediatrics. (2012). The lifelong effects of early childhood adversity and toxic stress. *Pediatrics*, 129(1), e232–e246. https://doi.org/10.1542/peds.2011-2663

Solove, D. (2021). The myth of the privacy paradox. *George Washington Law Review*, 89(1), 1–51.

Third, A., Collin, P., Walsh, L., & Black, R. (2019). *Young people in digital society: Control shift*. Palgrave Macmillan.

United Nations. (1989). *Convention on the Rights of the Child. United Nations Treaty Series*, 1577, 3.

United Nations. (2006). *Convention on the Rights of Persons with Disabilities*. United Nations Treaty Series, 2515, 3.

United Nations Committee on the Rights of the Child. (2009). *General Comment No. 12 (2009): The right of the child to be heard* (CRC/C/GC/12). United Nations.

United Nations Committee on the Rights of the Child. (2013). *General Comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration* (CRC/C/GC/14). United Nations.

United Nations Committee on the Rights of the Child. (2021). *General Comment No. 25 (2021) on children's rights in relation to the digital environment* (CRC/C/GC/25). United Nations.

van der Kolk, B. (2014). *The body keeps the score: Brain, mind, and body in the healing of trauma*. Viking.

Wright, D., & De Hert, P. (Eds.). (2012). *Privacy impact assessment*. Springer. https://doi.org/10.1007/978-94-007-2543-0