Children's Privacy in the Digital Age: US and UK Experiences and Policy Responses

Sonia Livingstone, Eva Lievens, Richard Graham, Kruakae Pothong, Stacey Steinberg, and Mariya Stoilova

1 Background

Children's privacy can receive culturally diverse interpretations and its implementation is often contested. To psychologists, it is vital to child development [1]. To clinicians, it is necessary for mental health. In the United Nations Convention on the Rights of the Child (UNCRC), it is a child's right. Yet, there is little consensus on from or by whom children's privacy should be protected. At issue are the dimensions of privacy (bodily, locational, communicational, decisional, and informational) [2], cultural understandings of privacy, and privacy's embedding in different legal systems [3, 4]. In most countries, legal protections center on privacy from the state, although also from commercial actors. Meanwhile, the public typically thinks of privacy in interpersonal terms, relying on negotiating social norms to protect their privacy.

In the digital age, privacy from the state, businesses, and individuals is both enabled and threatened by digital technologies and new forms of data processing, notably by commercial providers of digital products and services. Digital networks create new opportunities for interpersonal expression and exchange. These are highly valued by children and young people, although navigating digital spaces can make children's activities more visible to others than they realize [5]. However, privacy infringements are intensified now that everyday digital activities are tracked, shared, aggregated, and often monetized [6].

Data processing influences both privacy and the outcomes that depend on privacy—identity, dignity, freedom of thought and speech, safety, sociality, and participation. UNICEF argues that technological innovation impacts multiple dimensions of children's privacy and can have various negative effects [7]. Children's bodily (or physical) privacy is violated when tracking, monitoring, or live broadcasting or streaming technologies reveal a child's image, activities, or location. Their communicational privacy is violated when surveillant governments, bad actors, or unintended audiences gain access to children's posts, chats, or messages. Their informational privacy is violated when their personal data is

S. Livingstone (✉)
London School of Economics and Political Science, London, UK

Good Thinking: The London Digital Mental Wellbeing Service, London, UK
e-mail: S.Livingstone@lse.ac.uk

E. Lievens
Ghent University, Ghent, Belgium

R. Graham
stem4, London, UK

K. Pothong · M. Stoilova
London School of Economics and Political Science, London, UK

S. Steinberg
University of Florida, Gainesville, FL, USA

D. A. Christakis, L. Hale (eds.), *Handbook of Children and Screens*,
https://doi.org/10.1007/978-3-031-69362-5_67

collected, processed, or shared unlawfully or beyond what children reasonably expect. Finally, their decisional privacy is violated when digital design or automated decision making limits, directs, or biases children's thoughts and choices [8, 9].

In public and policy debates over privacy, children occupy an uneasy position. Media headlines complain that children's social media activities show they have no sense of privacy, also criticizing parents for publicly sharing images of their children. Parents, caregivers, and health advocates argue that children's privacy should not be invaded by commercial interests such as advertising and marketing [10]. Yet children's privacy gets short shrift in policy deliberations regarding privacy and data protection regulation. When it is discussed, it is often under the guise of keeping children safe rather than ensuring their right to privacy is honored [11]. Moreover, the same adults who defend their own privacy from the state and commerce may doubt that children need privacy, especially from their parents, notwithstanding that parental actions are not always in their child's best interests.

2 Current State

Privacy is widely theorized as relational, being variously sustained or threatened through social interactions shaped by conventions of visibility, intimacy, publicness, surveillance, consent, and redress. In highlighting these normative contextual factors, US legal scholar Helen Nissenbaum argues that privacy is "neither a right to secrecy nor a right to control, but a right to appropriate flow of personal information" [12]. How does, and how could, this apply in the digital environment, where children have little agency regarding the flow of their personal information (i.e., information that identifies them, either directly or indirectly)?

Research shows that children care about their privacy online, making efforts to create and sustain digital spaces that are both meaningful to them and privacy preserving, and finding tactics and workarounds when privacy settings are insufficient for their needs [13]. Yet the operation and consequences of the complex and opaque digital ecosystem in which children are increasingly immersed may remain beyond their comprehension, as they do for most adults. Hence, adequate policy responses are vital to protect children's privacy.

Unlike the right to free expression, the right to privacy is not an enumerated right within the text of the United States Constitution. As such, in the United States, courts will not weigh an individual's right to privacy equally with another individual's right to free expression or speech. Moreover, a parent's right to raise their child as they see fit is recognized as a constitutional right under the due process clause of the 14th Amendment. Thus, any discussions centered on a child's right to privacy are often outweighed both by parental rights to free expression and the parental right to dictate how the child is raised [14]. Laws that affect children's privacy either stem from a consumer or market perspective [15] (such as the 1998 Children's Online Privacy Protection Act (COPPA)), which requires parental consent for companies' processing of the data of children younger than 13, or they are adopted at the state level (such as the California Age-Appropriate Design Code Act). Recent legislative proposals by US lawmakers focus on children's online safety. While this may ultimately protect their privacy, it does not recognize children's agency according to their evolving capacities, which is recognized in the rights-based privacy protection in the UK and EU [16].

In the UK, and Europe more widely, although the right to privacy and the right to the protection of personal data are closely interlinked, they are not identical in scope or implementation [17]. Whereas the right to privacy prohibits state interference with an individual's personal sphere and the shaping and expression of identity (including sexual orientation) and family life, subject to some exceptions, the right to data protection provides a system of checks and balances for how information about an individual is processed by public and private actors [18]. The EU General Data Protection Regulation (GDPR), on which the UK data protection framework is also

grounded, acknowledges that data protection is closely linked to other fundamental rights, and that children's data merits heightened protection because of their vulnerability. In the UK, such protections for children are articulated through a legally binding Age Appropriate Design Code (AADC), now also adopted and considered in various forms internationally, including in California, Maryland, New Mexico, Argentina, and Indonesia.

Contexts in which tensions between child rights or between child and adult rights are particularly relevant are the family, health, and educational contexts.

2.1 The Family Context

Courts in the US are reluctant to regulate family matters, and parents in the US have significant legal protections to control the upbringing of their children. Meanwhile, children in the UK benefit from the rights afforded to them through several UK laws, underpinned by the UK's ratification of the UNCRC, which recognizes the need to respect children's evolving autonomy, capacities, and privacy, even when parents' and children's interests conflict. The US has not ratified the UNCRC, mainly due to the concern that it will undermine parental authority to discipline children and, more generally, raise children as parents see fit. Consequently, until a young person's eighteenth birthday, parents have the authority to disclose a young person's private information with minimal or no state intervention [19]. Even when courts recognize that young people have an interest in privacy, this interest traditionally ends where intrafamilial life begins. Consider the context of parents sharing information online about their children ("sharenting") [20]. While this may benefit parents socially and financially, it can jeopardize their child's privacy, and allow third parties to collect and further share children's data, including sensitive images or location information, in ways unintended or unanticipated by the parent and potentially harmful to the child [21].

It is almost inconceivable to imagine courts in the US enjoining parents from posting publicly about their children, except in the most limited circumstances. Indeed, parents in the US often share images with unfettered restraint due to cultural and legal expectations of parental autonomy and free speech. By contrast, the UNCRC, UK GDPR, and other laws applicable in the UK and Europe offer young people certain legal remedies. Under the European Convention of Human Rights, to which the UK is a party, conflicts between a parent's right to family life and expression and a child's right to privacy is assessed on a case-by-case basis by the European Court. This is done using the child's best interests (UNCRC Article 3.1) as a guiding principle when balancing parents' and children's rights. Further, parental disclosures, labeled speech in the US, may constitute personal data in the UK, affording children greater legal protections such as the right to ask for the erasure of images ("the right to be forgotten"). However, in practice, it is difficult for children to exercise their right to privacy, in particular against a parent, and especially when very young [22]. Furthermore, there are doubts whether sharenting falls within the household exemption, thereby rendering the GDPR inapplicable [23].

2.2 The Educational Context

Data are collected from children throughout their learning lives—at school and in nonformal and informal learning settings—in ways that are intensified by the reliance on educational technologies for teaching, safeguarding, and administration. The data collected are often sensitive (including race/ethnicity, family hardship, mental health, and disabilities) and can be analyzed to reveal further intimate details about each child. Whether data collection is mandated by the government or is a matter of school choice, it is likely that children's data enter a global commercial ecosystem extending far beyond the school [24]; meanwhile the promised benefits (resulting from personalized learning or learning analytics) do not always materialize [25].

In the United States, the federal law intended to protect the privacy of students' educational records is the Family Educational Rights and Privacy Act (FERPA). Designed to prevent misuse of students' records, FERPA prioritizes informational privacy and relies on parental consent as "the primary mechanism for disclosure" [26]. This puts the primary responsibility for protecting children's data on parents rather than businesses, although whether parents can provide meaningful consent in complex data-driven economies is questionable [27]. In December 2023, the Federal Trade Commission proposed changes to COPPA which could also affect education technology (EdTech) providers, including a prohibition to use children's information for commercial use and additional safeguards [28].

In the United Kingdom, children's personal data are protected by the UK Data Protection Act 2018 and the UK GDPR. Further, the AADC applies to EdTech services likely to be accessed by children on a direct-to-consumer basis (on the web or through an app) [29]. This ensures privacy-by-design, data minimization requirements, and data subject rights. In practice, however, the US and the UK share similar problems of compliance and enforcement, partly because children's privacy at school is commonly a low priority and use of tech is often not a (real) choice, and partly because schools lack the expertise and resources to hold powerful EdTech companies to account [30].

2.3 The Health Context

Privacy is core to the delivery of healthcare, which increasingly has a digital dimension. Data protection laws apply to health records, given the sensitive personal data they contain. In the United States, the Health Insurance Portability and Accountability Act (HIPAA) includes stringent information security standards. However, as with education, commercial technologies increasingly provide the infrastructure for health services delivery. While detailed consideration has been applied to children's capacity to consent to medical treatment, their options to consent (or not) to the consequent data processing are limited, even though the data at issue may be highly sensitive. With innovation in digitally facilitated treatment [31], concerns are growing regarding whether digital health services respect children's privacy and protect their data [32, 33]. In addition to data protection considerations, "confidentiality concerns can be a critical barrier for young patients in seeking and receiving appropriate medical services, and confidentiality protection represents an important evidence-based practice in adolescent health care" [34]. Increasingly, these concerns intersect: parents may be informed of their child's treatment or learn of it through an insurance statement, for instance, in ways that the child does not anticipate or is not in their interest, compromising confidentiality for young patients [34].

In the United Kingdom, young people aged 16 and 17 are treated similarly to adults, presumed to have sufficient capacity to decide about their medical treatment and exercise their data protection rights, although assessing their capacity can be challenging [35, 36]. From the age of 13, children deemed mature enough to make such decisions can access online, and without parental consent, confidential sexual health services including contraception, testing for sexually transmitted infections, and advice on unplanned pregnancy [37]. This medical judgement is mirrored by data protection regulation: recognizing that children increasingly go online to access help or counseling services, the UK GDPR and the GDPR allow children under the age of consent to do so without obtaining parental consent for the processing of their personal data.

3 Future Research

Research on children's privacy and data protection is actively developing across multiple sectors. There are some pressing gaps in knowledge, including the effect of video cameras, smart monitoring, or facial recognition in homes, schools, and public spaces, or of sharing sensitive or biometric data with health services or law enforcement.

Also important are knowledge gaps regarding how children of different ages and life circumstances understand and value their privacy, at home, with peers, and in relation to education, health, business, and other organizations. Research could examine whether unfolding privacy beliefs and practices affect children's online identity expression or agency or help-seeking, and whether this varies by dimensions of vulnerability.

Efforts to protect children's privacy raise new research questions in turn. How is existing legislation enforced, and which new policies and practices are emerging to protect children's privacy, and are they effective? What mechanisms would incentivize service providers to implement necessary safeguards? Also, are efforts to increase digital literacy, even to resist the datafication of children's lives, proving effective?

Finally, research could examine whether the global nature of big tech is harmonizing cultural understandings of children's privacy or provoking divergent responses in different countries or contexts (such as law, education, health, or welfare). Related, are strategies emerging to enable children to benefit from the data collected from them? Indeed, what role do and could children play in shaping future policy responses?

Such questions are especially pressing as artificial intelligence (AI) becomes more pervasive in contexts (education, health, transport), where dependence on technical systems means neither children nor parents have meaningful opportunities to give or withdraw consent or exercise other rights. However, the present chapter suggests a sufficient evidence base for clear recommendations, as below.

4 Recommendations

- Government policies on privacy and data must promote children's rights, facilitating their need for protection and participation, and prevent discrimination and other harms arising from privacy violations and data exploitation in digital contexts. Governments should also involve young people in the policymaking process, by giving children real agency in influencing decisions that affect them, including policy and product design.
- There must be necessary safeguards in place for children's privacy and data protection when data- and AI-driven technologies are used in public services affecting or used by children (notably education, health, and welfare). In addition, these safeguards need to be regularly updated to keep pace with technological innovation.
- Since neither children nor families can realistically be held solely responsible for navigating the complex, global, and largely commercial digital environment on which their lives increasingly depend, the government must regulate or legislate robust standards of privacy by design and by default, as included in the UK Data Protection Act and AADC, and ensure that big tech provides child-friendly, age-appropriate mechanisms for privacy protection, transparency, complaint, and remedy.
- Sustained media (data, digital, privacy critical, AI) literacies are vital from an early age. They should be implemented in school curricula, professional training (for teachers, clinicians and other professionals who work with children), and parent/caregiver guidance. Such initiatives should be informed by children's voices, reflect their concerns and experiences, and respond to real-world problems.
- A robust evidence base must be sustained that fills critical gaps, especially regarding younger children and those living in vulnerable or disadvantaged situations, provides an independent evaluation of the effectiveness of privacy-related interventions, and consults children for their own experiences and views.

Conflict of Interest and Funding Disclosures None.

References

1. Laufer R, Wolfe M. Privacy as a concept and a social issue: a multidimensional developmental theory. J Soc Issues. 1977;33(3):22–42.
2. Koops B-J, Newell BC, Timan T, Škorvánek I, Chokrevski T, Galič M. A typology of privacy. Univ

Pa J Int Law. 2017;38(2):483–57. Available at: https://scholarship.law.upenn.edu/jil/vol38/iss2/4. Accessed 2 May 2023.
3. Livingstone S, Lemish D, Lim SS, Bulger M, Cabello P, Claro M, Cabello T, Khalil J, Kumpulainen K, Nayar U, Nayar P, Park J, Tan M, Prinsloo J, Wei B. Global perspectives on children's digital opportunities: an emerging research and policy agenda. Pediatrics. 2017;140(2):137–41. https://doi.org/10.1542/peds.2016-1758S.
4. Livingstone S, Bulger M, Burton P, Day E, Lievens E, Milkaite I, Leyn T, Martens M, Roque R, Sarikakis K, Stoilova M, Wolf R. Children's privacy and digital literacy across cultures: implications for education and regulation. In: Sefton-Green J, Pangrazio L, editors. Learning to live with datafication: educational case studies and initiatives from across the world. Abingdon: Routledge; 2022. p. 184–200.
5. Milkaite I, De Wolf R, Lievens E, De Leyn T, Martens M. Children's reflections on privacy and the protection of their personal data: a child-centric approach to data protection information formats. Child Youth Serv Rev. 2021;129:106170. Available at: https://doi.org/10.1016/j.childyouth.2021.106170. Accessed 2 May 2023.
6. Mascheroni G, Siibak A. *Datafied childhoods: data practices and imaginaries in children's lives*. New York, London: Peter Lang; 2021. Available at: https://doi.org/10.3726/b17460. Accessed 2 May 2023.
7. UNICEF (United Nations Children's Fund). Children's online privacy and freedom of expression. 2018. Available at: www.guvenliweb.org.tr/dosya/ZybsG.pdf. Accessed 2 May 2023.
8. Alegre S. Freedom to think: the long struggle to liberate our minds. London: Atlantic Books; 2022.
9. Eubanks V. Automating inequality: how high-tech tools profile, police, and punish the poor. New York: St. Martin's; 2018.
10. Radesky J, Chassiakos YR, Ameenuddin N, Navsaria D. Digital advertising to children. Pediatrics. 2020;146(1):e20201681. Available at: https://doi.org/10.1542/peds.2020-1681. Accessed 2 May 2023.
11. Lievens E, Livingstone S, McLaughlin S, O'Neill B, Verdoodt V. Children's rights and digital technologies. In: Liefaard T, Kilkelly U, editors. International children's rights law. Singapore: Springer; 2018. p. 1–27.
12. Nissenbaum H. Privacy in context: technology, policy, and the integrity of social life. Stanford: Stanford University Press; 2010. p. 3.
13. Stoilova M, Nandagiri R, Livingstone S. Children's understanding of personal data and privacy online—a systematic evidence mapping. Inf Commun Soc. 2021;24(4):557–75. Available at: https://doi.org/10.1080/1369118X.2019.1657164. Accessed 2 May 2023.
14. Milkaite I, Lievens E. Children's rights to privacy and data protection around the world: challenges in the digital realm. Eur J Law Technol. 2019;10(1):1–24.
15. Schwartz PM, Peifer KN. Transatlantic data privacy law. Georgetown Law J. 2017;106(1):115–80.
16. Lynskey O. The foundations of EU data protection law. Oxford: Oxford University Press; 2015.
17. González Fuster G. Study on the essence of the fundamental rights to privacy and to protection of personal data. 2022. https://www.edps.europa.eu/system/files/2023-11/edps-vub-study_on_the_essence_of_fundamental_rights_to_privacy_and_to_protection_of_personal_data_en.pdf
18. FRA (European Union Agency for Fundamental Rights), Council of Europe. Handbook on European data protection law. Luxembourg: Publications Office of the European Union; 2018.
19. Shmueli B, Blecher-Prigat A. Privacy for children. Columbia Hum Rights Law Rev. 2010;42:759.
20. Steinberg S. Growing up shared: how parents can sharer smarter on social media and what you can do to keep your family safe in a no-privacy world. Naperville: Sourcebooks; 2017.
21. Blum-Ross A, Livingstone S. "Sharenting," parent blogging and the boundaries of the digital self. Pop Commun. 2017;15(2):110–25.
22. ICO. What rights to children have? https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/what-rights-do-children-have/.
23. Bessant C, Schnebbe M. Does the GDPR offer a solution to the "problem" of sharenting? Datenschutz Datensich. 2022;46:352–6. https://link.springer.com/article/10.1007/s11623-022-1618-3.
24. Livingstone, S., Pothong, K., Atabey, A., Hooper, L., & Day, E. (2024) The Googlization of the classroom: Is the UK effective in protecting children's data and rights? Computers and Education Open. https://doi.org/10.1016/j.caeo.2024.100195
25. Selwyn N, Hillman T, Bergviken Rensfeldt A, Perrotta C. Digital technologies and the automation of education—key questions and concerns. Postdigital Sci Educ. 2023;5:15–24. Available at: https://doi.org/10.1007/s42438-021-00263-3. Accessed 2 May 2023.
26. Vance A. Lessons learned from the Family Educational Rights and Privacy Act. In: Livingstone S, Pothong K, editors. *Education data futures: critical, regulatory and practical reflections*. London: 5Rights Foundation; 2022. p. 189–201. Available at: https://educationdatafutures.digitalfuturescommission.org.uk/essays/the-value-of-better-regulation/lessons-learned-from-the-famuly-educational-rights-privacy-act. Accessed 2 May 2023.
27. Edwards L. Privacy, security and data protection in smart cities: a critical EU law perspective. Eur Data Prot Law Rev. 2016;2(1):28–58.
28. FTC. FTC proposes strengthening children's privacy rule to further limit companies' ability to monetize children's data. https://www.ftc.gov/news-events/news/press-releases/2023/12/ftc-proposes-strengthening-childrens-privacy-rule-further-limit-companies-ability-monetize-childrens.
29. ICO. The children's code and education technologies (edtech). https://ico.org.uk/for-organisations/uk-

gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/the-childrens-code-and-education-technologies-edtech/.
30. Day E, Pothong K, Atabey A, Livingstone S. Who controls children's education data? A socio-legal analysis of the UK governance regimes for schools and EdTech. Learn Media Technol. 2022;49:356–70. Available at: https://doi.org/10.1080/17439884.2022.2152838. Accessed 2 May 2023.
31. Hollis C, Livingstone S, Sonuga-Barke E. Editorial: the role of digital technology in children and young people's mental health—a triple-edged sword? J Child Psychol Psychiatry Allied Discip. 2020;61(8):837–41.
32. Grundy Q, Jibb L, Amoako E, Fang GH. Health apps are designed to track and share. Br Med J. 2021;373:n1429. https://doi.org/10.1136/bmj.n1429.
33. Bahareh K, Steinberg S. Parental sharing on the internet: child privacy in the age of social media and the pediatrician's role. JAMA Pediatr. 2017;171(5):413–4. https://doi.org/10.1001/jamapediatrics.2016.5059.
34. Pathak PR, Chou A. Confidential care for adolescents in the U.S. health care system. J Patient Cent Res Rev. 2019;6(1):46–50. https://doi.org/10.17294/2330-0698.1656. PMID: 31414023; PMCID: PMC6676754.
35. GMC (General Medical Council). Confidentiality: good practice in handling patient information. London: GMC; 2017 [updated 2018].
36. GMC (General Medical Council). l0–18 years: guidance for all doctors. London: GMC; 2007 [updated 2018].
37. NHS England. Sexual health. 2022. Available at: www.nhs.uk/live-well/sexual-health/confidentiality-at-sexual-health-services. Accessed 2 May 2023.