University of Southampton

HARMFUL SHARENTING IN THE UK

Protecting children from digital harm

Context

Sharenting - the sharing of children's personal information by parents on social media - has become a widespread practice. While often well-intentioned, it exposes children to digital harm. Examples include identity-related crimes, harassment, cyberbullying, contact from strangers, and privacy breaches.

Funded by the Economic and Social Research Council (ESRC), and led by researchers at the University of Southampton, the ProTechThem interdisciplinary research project brings together social and computer science expertise to investigate whether and how sharenting leads to serious (cyber) crimes and harms against affected children.

The project reveals that current regulations, platforms' safety provisions, and parental cybersecurity measures are insufficient to protect affected children from harm. This brief outlines victimisations experienced by children due to sharenting and proposes actionable policy recommendations for a safer digital future.

Key messages

Parental Awareness and Misplaced Trust in Platforms: Our survey of a nationally representative sample of 1013 UK parents with children under 18 found a major gap in cybersecurity awareness, with many parents overestimating platform safeguards such as private settings.

- 82.7% of sharers set their account to 'private' when sharing about their children online.
- Despite the use of this privacy setting, there was no statistically significant difference in rates of reported child cybervictimisation across private and public account users.
- Two key themes emerged from interviews with 30 UK parents: poor parental awareness that the privacy setting provided by platforms is not fully secure, and inaccessible platform policies on how to manage digital risks.

Children's Rights and Digital Exposure: Children's rights to an identity, autonomy, and privacy under Articles 8, 12, and 16 of the United Nations Convention on the Rights of the child (UNCRC) are often unintentionally violated through online disclosures.

- The project's digital ethnography of social media groups found that parents reveal personal and sensitive information about their children (such as images, location, and birth date) which can be misused by malicious actors to harm children.

Weak Platform Accountability and Regulatory Gaps: Social media platforms lack robust privacy-by-design mechanisms involving the integration of data security measures. Robust privacy settings, pop ups or other reminders when sharing images of children are examples. Legal frameworks such as The Online Safety Act 2023, The UK General Data Protection Regulation - GDPR, and the Data (Use and Access) Act 2025, do not specifically address the risks that sharenting poses to children, leaving regulators, educators, and parents without clear guidance.

Key findings

45%

Prevalence:
45% of UK parents practice sharenting

Commonly used platforms:
Facebook, Instagram, TikTok

Data shared:
Children's photos, names, birthdate, health conditions, location, school milestones, school-related difficulties, and emotional problems.

1/6

Victimisation
1 in 6 reported negative incidents affecting children (identity-related crimes, cyberbullying, contact from strangers, and privacy breaches).

Implications:
The victimisations are direct harms (e.g. harassment, cyberbullying, and contact from strangers) or data-related crimes (identity-related crimes and privacy breaches).
These pose longer term social, psychological, and financial risks for children.

- Social risks such as damaged online and digital identities can arise when for example, children's images are misused for generating deepfakes or for digital kidnapping where predators steal the images and post it as theirs or pass the children off as their own. This can have long term reputational consequences for the affected children. Psychological risks can include mental distress due to victimisation. Financial risks stem from opportunities to hack into bank accounts using the information that parents share about their children on social media.

False sense of security:
Parents overestimate the effectiveness of platforms' privacy settings and are unaware of how platforms enable or constrain their ability to manage digital risks whilst sharenting.

Sharenting practices associated with higher levels of cybervictimisation against children:
Weak cybersecurity measures devised by parents and frequent sharing.

Platform vulnerabilities:
Easy re-shareability of children's information across social media, inaccessible privacy policies.

Typology of sharenting harms affecting children

- Identity fraud
- Identity theft
- Harassment
- Cyberbullying
- Contact from strangers
- Unauthorised sharing of children's personal data

Recommendations

Policy Makers, regulators, and legislators:

1. **Establish a Coordinated UK Risk Mitigation Strategy:** Convene a multi-stakeholder taskforce including Ofcom, DCMS, ICO, Children's Commissioner, NGOs, and schools; Embed children's rights into digital parenting guidance, modelled on Articles 8, 12, & 16 of the UNCRC.
2. **Strengthen Platform Responsibilities:** Mandate the sharing of child-specific content to be private-by-default; Mandate platform data protection audits focusing on personal and sensitive child-specific content (images and other information); Mandate platforms to publish annual data on sharenting-related incidents; Require platforms to publish plain-language safety notices or pop-ups during child content uploads. Mandate platforms to restrict the ability of others to repost or screenshot the content that parents share about their children.
3. **Build Parental Cybersecurity Awareness:** Integrate ProTechThem's animated risk awareness video and the Sharenting Risk Awareness Checklist (available at: https://www.protechthem.org) into national online safety curricula and parenting classes; Support co-branded campaigns between schools, NGOs, and tech companies.
4. **Regulate Criminogenic Affordances:** Expand the Online Safety Act to explicitly include sharenting-related harms; Ban platform practices that algorithmically amplify child-centric content to inappropriate audiences.
5. **Create an Independent Ombudsman for Child Data Harms:** Establish a Children's Data and Privacy Ombudsman, empowered to receive complaints, advise families, and issue guidance to platforms and other digital service providers. The existing Local Government and Social Care Ombudsman focuses on child protection issues and Ofcom, the UK's independent media regulator, does not provide the proposed service.
6. **Introduce centralised control:** Bring sharenting under the oversight of the Children's Commissioners for England and Wales.
7. **Invest in Interdisciplinary Sociotechnical Tools:** Fund development and deployment of AI tools for sharenting risk detection; Encourage platform adoption of automated moderation systems: These can flag sensitive child-related posts. The ProTechThem interdisciplinary research team have designed an open-source AI system based on Large Language Models (LLMs). The team have also developed a digitised cybersecurity awareness checklist for parents and an animated risk awareness video.

Police:

8. Train police & social workers on digital harms and privacy rights under legislation such as the UK GDPR, the Data Protection Act, and the UNCRC.

Educators:

9. Incorporate sharenting risk awareness into school ICT curricula: Collaborate with Ofsted
10. Train teachers and parents on digital harms and privacy rights
11. Review Schools' use of social media in line with our findings and recommendations
12. Resources available at the project's website (https://www.protechthem.org) can be integrated into staff training, school ICT teaching, and social media policies.

Service Providers:

13. Embed proactive pop-ups/reminders that are triggered by child-centric uploads.
14. Perform audits on data protection mechanisms for children affected by sharenting.
15. Publish annual data on sharenting-related incidents.
16. Partner with law enforcement and NGOs to test and refine automated risk detection systems; Develop a what across-sectoral taskforce to monitor tech developments and associated risks.

Citation:

Ugwudike, P., Roth, S., Lavorgna, A., Middleton, S. E. and Djohari, N. (2025) Harmful sharenting in the UK: Protecting children from digital harm, Policy Brief, University of Southampton, **DOI:** doi.org/10.5258/SOTON/PP0117

Lead Researchers

Prof Pamela Ugwudike | University of Southampton
Prof Silke Roth | University of Southampton
Professor Stuart E. Middleton | University of Southampton
Dr Anita Lavorgna | University of Bologna

Research Fellows

Dr Natalie Djohari | University of Southampton
Dr Morena Tartari | University of Southampton (2021-2022)
Dr Arpan Mandal | University of Southampton (2022-2024)
Junyu Mao | University of Southampton

Research Assistant

Yijia Gao | University of Southampton

Contact:

Find out more

ProTechThem: Building Awareness for Safer and Technology-Savvy Sharenting
www.protechthem.org

Contact

Email: **p.ugwudike@soton.ac.uk**

This policy brief draws on interdisciplinary research funded by ESRC [ES/V011278/1] conducted by researchers at the University of Southampton. The UK's DCMS, NGOs, and child safety organisations contributed to various stages of the project.