



Children's conception of privacy online

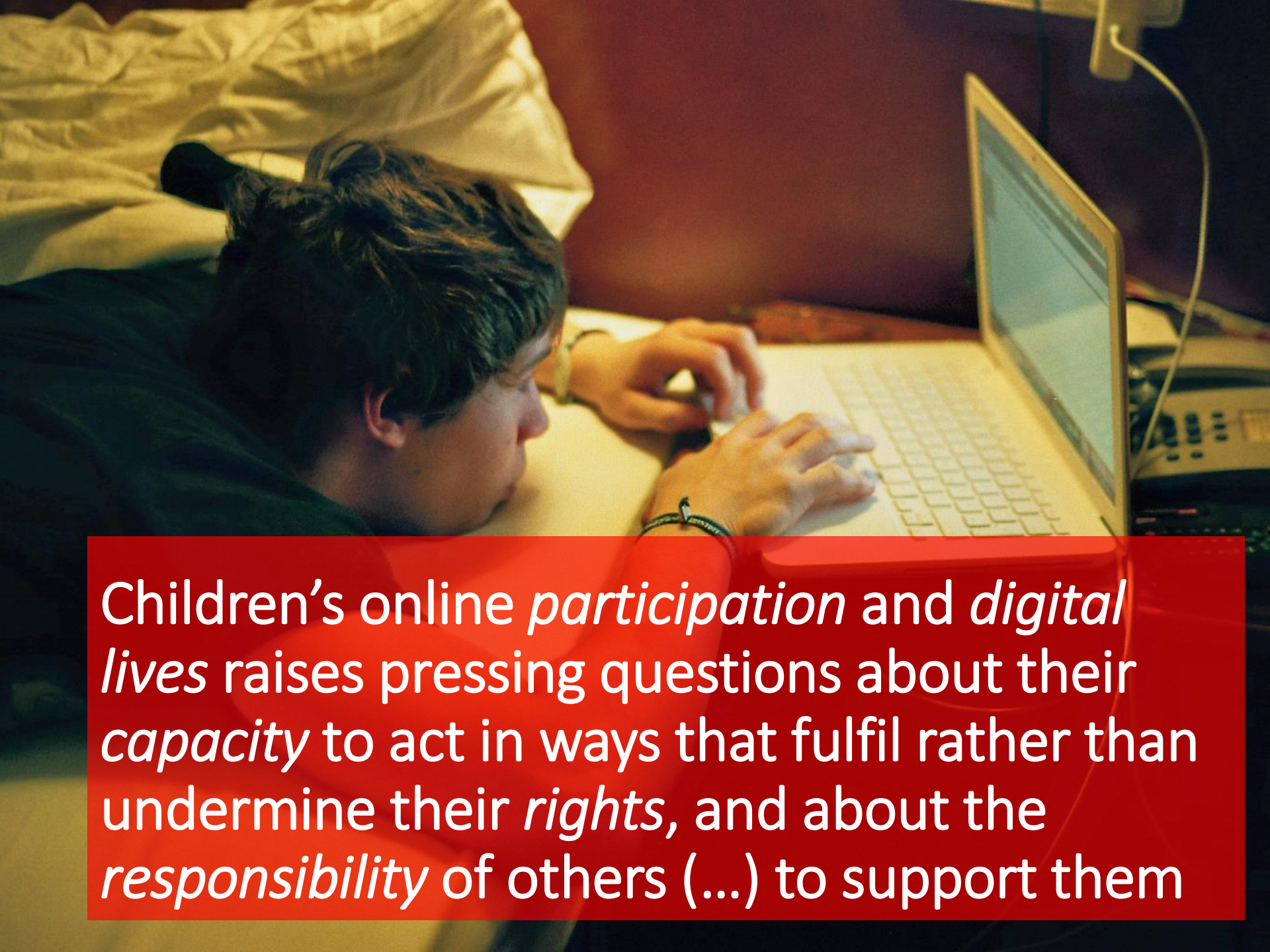
Sonia Livingstone, Mariya Stoilova & Rishita Nandagiri
@Livingstone_S
s.livingstone@lse.ac.uk
www.sonialivingstone.net

LSE

Department of
**Media and
Communications**

ico.
Information Commissioner's Office

Grant
Recipient

A young man with dark hair is lying on his stomach on a bed, using a laptop. He is wearing a dark green shirt and a black watch on his left wrist. The laptop is open, and he is typing on the keyboard. The background is a white pillow and a dark headboard. The scene is dimly lit, with the laptop screen providing the main source of light.

Children's online *participation* and *digital lives* raises pressing questions about their *capacity* to act in ways that fulfil rather than undermine their *rights*, and about the *responsibility* of others (...) to support them



Article 16

1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.
2. The child has the right to the protection of the law against such interference or attacks.

- (38) Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

- “Neither a right to secrecy nor a right to control, but a right to appropriate flow of personal information”
- Privacy is vital for autonomy, identity, trust, participation, development, and well-being – as both means and end (as in 2012 OECD typology of risks)
- The digital environment continually reconfigures practices, opportunities and risks, thereby challenging understanding





Guidelines to respect, protect and fulfil the rights of the child in the digital environment



www.coe.int/children

Building a Europe
for and with children



3.4. Privacy and data protection

26. Children have a right to private and family life in the digital environment, which includes the protection of their personal data and respect for the confidentiality of their correspondence and private communications.

27. States must respect, protect and fulfil the right of the child to privacy and data protection. States should ensure that relevant stakeholders, in particular those processing personal data, but also the child's peers, parents or carers, and educators, are made aware of and respect the child's right to privacy and data protection.

28. States and other stakeholders should ensure that children are made aware of how to exercise their right to privacy and data protection, taking into account their age and maturity and, where appropriate, with the direction and guidance of their parents, carers, legal guardians or other persons legally responsible for the child in a manner consistent with the evolving capacities of the child.

29. Recognising that personal data can be processed to the benefit of children, States should take measures to ensure that children's personal data is processed fairly, lawfully, accurately and securely, for specific purposes and with the free, explicit, informed and unambiguous consent of the children and/or their parents, carer or legal representative, or in accordance with another legitimate basis laid down by law. The data minimisation principle should be respected, meaning that the personal data processing should be adequate, relevant and not excessive in relation to the



Interpersonal
privacy

Institutional
privacy

Commercial
privacy



Interpersonal privacy

Data given

Data given off

Inferences

Institutional privacy

Data given

Data traces
(knowing)

Inferred data
(analytics)

Commercial privacy

Data given

Data traces
(taken)

Inferred data
(profiling)

Systematic evidence mapping:

- How do children understand, value and negotiate their privacy online?
- What are the capabilities and vulnerabilities with which children approach the digital environment?
- What are the significant gaps in knowledge about children's data and privacy online?
- Search: 19 databases yielded 9,119 search items + 270 expert suggestions
- Analysis: 130 empirical studies, 266 framing studies; report in progress

Interviews with children, parents, teachers ...





Differences among children

- Age / maturity / development
- Media (& other) literacies
- Socio-economic & other inequalities
- Resilience / vulnerability

5-7 years

Interpersonal privacy

- A developing sense of ownership, fairness and independence
- Learning about rules but may not follow, and don't get consequences
- Use digital devices confidently, for a narrow range of activities
- Getting the idea of secrets, know how to hide, but tend to regard tracking/monitoring as helpful



Institutional and Commercial Privacy

- Limited evidence on understanding of the digital world
- Low risk awareness (focus on device damage or personal upset)
- Few strategies (can close the app, call on a parent for help)
- Broadly trusting

8-11 years

Interpersonal privacy

- Starting to understand risks of sharing but generally trusting
- Privacy management means rules not internalised behaviour
- Still see monitoring positively, as ensuring their safety
- Privacy risks linked to 'stranger danger' and interpersonal harms
- Struggle to identify risks or distinguish what applies offline/online

Institutional and Commercial Privacy

- Still little research available
- Gaps in ability to decide about trustworthiness or identify adverts
- Gaps in understanding privacy terms and conditions
- Interactive learning shown to improve awareness and transfer to practice

12-17 years

Interpersonal privacy

- Online as 'personal space' for expression, socialising, learning
- Concerned about parental monitoring yet broad trust in parental and school restrictions
- Aware of / attend to privacy risks, but mainly seen as interpersonal
- Weigh risks and opportunities, but decisions influenced by desire for immediate benefits

Institutional and Commercial Privacy

- Privacy tactics focused on online identity management not data flows (seeing data as static)
- Aware of 'data traces' (e.g. ads) and device tracking (e.g. location) but less personally concerned nor aware of future consequences
- Willing to reflect and learn retrospectively; media literacy education best if teens can use new knowledge to make meaningful decisions

Recommendations

- Child-rights-respecting policies for the digital environment are needed to balance protection and autonomy, and prevent discrimination and long-term consequences
- Sustained media (data, digital, critical) literacy education from an early age is vital, but not a “silver bullet”
- Support children by supporting parents, teachers, welfare bodies able to address “best interests” and vulnerabilities
- Privacy-by-design, mechanisms for redress, enforcement, evaluation all important, and should be informed by strong evidence base and children’s voices



Sources

- Council of Europe. (2018) New Recommendation adopted on children's rights in the digital environment
<https://www.coe.int/en/web/children/-/new-recommendation-adopted-on-children-s-rights-in-the-digital-environment>
- Livingstone, S. (2018) The value of children's privacy in the regulation of personal data protection. *InterMedia*, 46(2): 18-23.
<http://www.iicom.org/intermedia/intermedia-july-2018/children-a-special-case-for-privacy>
- Children's Data and Privacy Online project website <http://www.lse.ac.uk/media-and-communications/research/research-projects/childprivacyonline>
- van der Hof, S. (2016) I agree, or do I: a rights-based analysis of the law on children's consent in the digital world *Wisconsin International Law Journal* 34: 409-445.