



Children AND Screens

INSTITUTE OF DIGITAL MEDIA AND
CHILD DEVELOPMENT

Research at a GLANCE

DATA PRIVACY and CHILDREN

2023

Children's data is vulnerable when using any internet-enabled digital or smart product
(phone, toy, tablet, laptop, computer)



SMART TOYS

Name

Gender

Sex

Birth data

Parent names

Mailing address

Email address

"Secret questions" and answers

IP address

Download history

Encrypted passwords



VIDEO GAMES

Financial data from
in-game purchases

Behavioral data

(player movements, purchases,
amount of time spent doing tasks,
how they interact with game
elements)

Physical location

Email address

ISP

Camera access



SOCIAL MEDIA
PLATFORMS

Locations

Browsing history

Images

Videos

Contacts

Messages

Behavioral data

(what posts are viewed, how long
they are viewed, etc)

Data shared by parents



SEARCH
ENGINES

Locations

Browsing history



EDUCATIONAL
SOFTWARE

Email address

Passwords

Online activity

Biometric data

Religion

Heritage

Date of birth

Sexual orientation

Ability/Disabilities

Family income range

Data collected from children may be stored, sold to third parties, given, sold to, or seized by governments, shared with advertisers, used for marketing, and for a host of other purposes.



(Burgess, 2021; Fang, 2020; Foust & Jerome, 2021; Hecht-Felella, 2021; Henderson & American Bar Association, Criminal Justice Standards Committee, 2013; Kearsley-Ho, 2021; Kift & Nissenbaum, 2016; McCourt, 2019; Quayyum et al., 2021)

298

Number of known data breaches in 2022 from
different sectors only one of which included
exposing the data of millions of K-12 students
(2023 Third Party Data Breach Report 2023)

7.34

per day total recreational screen
time for adolescents
(Nagata et al., 2022)

WHY IT
MATTERS

3
OUT
OF 4

parents report sharing stories, images, or
videos of their children on social media
(Parents' Social Media Habits, 2021)

98%

of children ages 3-18 have access to a
computer or smartphone in their home
(National Center for Education Statistics, 2021, 2022)

WHAT DOES DATA PRIVACY MEAN TO CHILDREN?



0-5 years old



5-7 years old



8-11 years old



12-17 years old

Children

- cannot grasp privacy (or steps to protect it) in a meaningful way.
- are just starting to distinguish between self and others.

Children

- are developing a sense of interpersonal privacy, but are still generally trusting.
- have a very limited understanding of online privacy.
- don't always follow privacy rules, because they lack awareness of risk and consequences.

(Livingstone, Stoilova, & Nandagiri, 2019)

Children

- can follow privacy rules and understand some risks (i.e., personal harms), but have not internalized reasons why.
- have more difficulty managing online privacy settings and understanding privacy terms and conditions than teens.
- can benefit from interactive learning and the support of clear guidelines.

Adolescents

- are aware of privacy issues but less concerned with consequences. The knowledge of risk may be overshadowed by the benefits of connection and other immediate rewards.
- are more skilled at implementing strategies to protect personal privacy, but may still lack understanding of broader, commercial data uses.
- are generally trusting of platforms and their default settings.
- often focus privacy efforts on interpersonal privacy and identity management.
- can learn strong media literacy skills, which should build on existing knowledge, retrospective reflection, and direct application.

CLICK HERE FOR
RESEARCH CITATIONS



AND LEARN MORE
ABOUT OUR WORK

Note: These are general frameworks. Privacy understanding may vary according to a variety of individual cognitive, emotional, social, and cultural factors. Understanding may also vary according to types of privacy (interpersonal, institutional, and commercial), with mastery of interpersonal privacy generally coming before a broader understanding of institutional and commercial privacy issues.

KEY TAKEAWAYS

THE FUNDAMENTALS: Privacy isn't necessarily a complete control or restriction of personal information. Rather, it's a right to negotiate where, how, and when personal information flows between individuals and larger networks.

DEVELOPMENTAL STAGE MATTERS: Understanding and skills develop with age, but remain limited relative to the risks through adolescence. As knowledge grows, protecting privacy should move away from restriction and monitoring, and toward teaching and collaboration.

LEAD WITH EDUCATION: Often, children are capable of understanding certain privacy risks, but lack the awareness of those risks. Digital media literacy skills can be learned across childhood and adolescence, and should be scaffolded according to their current understanding.

INCREASED UNDERSTANDING AND TRANSPARENCY: Teaching appropriate privacy habits is difficult when even adults don't fully understand privacy issues and risks themselves. Resources and more manageable privacy terms and conditions need to be made available.

PROTECT CHILDREN'S DATA: Digital interactions and data tracking start early - protections and education must start early. Data is collected all the time, but protections around data and data flows are not always clear or strong enough.

RESPECT CHILDREN'S RIGHTS: Risks are broad and protections are few, especially for children over 13. Privacy is a basic right that all children under 18 should be granted.

(United Nations Convention on the Rights of the Child, 1989)

“With growing concerns over children's online privacy and the commercial uses of their data, it is vital that children's understandings of the digital environment, their digital skills and their capacity to consent are taken into account in designing services, regulation and policy.”

Sonia Livingstone,

DPhil (Oxon), OBE, FBA, FBPS, FAcSS, FRSA
Professor of Social Psychology,
The London School of Economics and Political Science
(Children's Data and Privacy Online, n.d.)



childrenandscreens.org

Helping children lead healthy lives in a digital world