

# Some children at higher risk of privacy violations from digital apps

8 September 2020



Credit: CC0 Public Domain

As your preschooler plays an alphabet game, does a puzzle or dresses up a favorite character through an app on a phone or tablet, companies may be stealthily collecting their personal information for marketing purposes.

Just like adults, children often leave [digital footprints](#) disclosing what websites they use and which games they play as well as data identifying their location and device.

Except their information is supposed to be off limits to advertisers.

But while [federal privacy laws](#) prohibit [digital platforms](#) from storing and sharing children's [personal information](#) without verifiable parental consent, those rules aren't always enforced, researchers find. And [privacy violations](#) are most likely to affect kids from lower-education households.

Children raised by parents without [college degrees](#) showed two to three times higher rates of digital information being transferred to third parties,

according to the study that appears in *JAMA Pediatrics*.

"Our study suggests that potential violations of child digital privacy laws are common, and social economic factors may influence which children are at greater risk for these violations," says senior author Jenny Radesky, M.D., developmental behavioral pediatrician and Michigan Medicine C.S. Mott Children's Hospital.

Potential factors that may explain this disparity include the degree of digital savviness or privacy awareness that parents have, authors say, which tends to correlate with level of education. Parents with advanced degrees also may research kids' apps before installing them, thereby avoiding the glut of lower-quality kids' apps in the app stores that could harbor more data trackers, Radesky says.

## Tracking children

Advertisers can learn a lot about consumers from how they spend time on smartphones and tablets, such as what they download or purchase, their location and frequently visited websites. For this reason, many apps collect device's unique identifiers (like Google's 'advertising ID' or 'Android ID' or even someone's location or email) and send them to third party marketing companies that analyze the data, combine it with data about the user from other sources, and deliver 'insights' about the user.

These techniques power the mobile advertising business.

Knowing that kids' apps often collect and share these identifiers, Radesky and colleagues analyzed 450 apps used by families with children ages three to five. Two-thirds of apps played by 124 preschool-aged children showed collection and sharing of persistent digital identifiers with large third party databases such as Facebook Graph, the primary

tool for getting information in and out of the Facebook platform.

For each app, researchers calculated the number of unique data transmissions detected and the number of third party domains involved.

The most commonly transmitted data included advertising identifiers (information used by advertisers to track users), followed by Android identifiers, hardware transmissions (i.e. device serial number) and geolocations.

Digital data for children under age 13 is protected under the Children's Online Privacy Protection Act. But enforcement of the law has mostly been limited to actions filed against large platforms like TikTok and YouTube.

Radesky notes that in previous research, parents and children have reported not understanding digital privacy concepts, including apps' collection practices, targeted advertising or how private information is stored.

"Consumers often don't know when digital data is being collected or shared with third party companies, which makes it difficult to make informed decisions about choosing apps for their children," Radesky says.

### **Better protection for children's digital privacy**

Older children and those with their own devices showed a high number of transmissions to third parties, but authors note that this may be because older children may be more likely to have their own devices and use a higher number of apps not intended for children.

This raises the question around whether general audience apps should consider younger audiences in their design, Radesky says. Children may easily download age-inappropriate apps from Google play when parent controls aren't enabled.

"App developers and platform designers play an important role in reducing or eliminating children's data collection from their products. This may be standard practice for tracking adults' behaviors,

which itself is ethically questionable, but it is off limits for kids," Radesky says.

Why does data collection matter? Radesky notes that, because of their developmental level, children don't understand the persuasion behind advertising and can't resist it.

"It's not fair to monitor kids' behavior to then serve them the perfectly crafted advertisement or in-app purchase, with the goal of monetizing their play," Radesky says.

"Play should not be surveilled by companies. Kids should be free to play without nudges or persuasion motivated by profit motives."

She notes that many of the digital identifiers that track users across apps are not needed to help apps function better. PBS KIDS for example created a novel identifier for each user that can't be traced back to their identity or across other apps, but still allows tracking of app functioning and use.

One of the study's limitations is that in homes with shared devices, researchers relied on parents reports of which apps their child uses—which may not always be accurate. The method the team used for measuring data transmissions also tends to underestimate their quantity, so results represent a minimum estimate of what the apps actually collected and shared.

"Our findings highlight the need for comprehensive testing of app and platform data collection practices by regulatory bodies," Radesky says. "We need more accurate information to better craft privacy legislation that adequately protects [children's](#) rights in the modern digital environment."

**More information:** *JAMA Pediatrics* (2020). [DOI: 10.1001/jamapediatrics.2020.3345](https://doi.org/10.1001/jamapediatrics.2020.3345)

Provided by University of Michigan

APA citation: Some children at higher risk of privacy violations from digital apps (2020, September 8) retrieved 30 October 2020 from <https://medicalxpress.com/news/2020-09-children-higher-privacy-violations-digital.html>

*This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.*