Where kids' information goes in an AI world

Understanding how tools collect data, privacy gaps, and why kids' information is so valuable

Tips for parents

Did you know?

Digital tools often collect a lot of information about kids. This might include names, birthdays, locations, time spent on the platform, or the type of phone or computer they use. These platforms can also track details from kids' conversations with chatbots, including information about their health, their interests, and their feelings.

When kids use any tool with AI, their data may be "harvested." Data harvesting is when tools using AI (e.g., chatbots, location trackers, smart speakers) automatically gather bits of information about users, such as where kids are, their health information, and what kids say, upload, or interact with. This information is collected each time a kid uses the tool and, over time, can form a detailed profile of their movements, preferences, feelings, and thoughts.

Technology companies can sell kids' information. Every company is different. Some keep kids' information private, while others share or sell it to businesses or government authorities. One company was reported to be selling the precise location of where your kid is.* Kids' information is valuable because it can be used to target kids with highly personalized advertisements, enticing them to buy or ask for certain products.

Some AI tools collect especially sensitive information. AI chatbots that are designed to act like friends or romantic partners, called AI companions, encourage frequent, personal interaction and are known for extensive data harvesting. One study found that these applications constantly gather personal information and described romantic AI companions as having some of the worst privacy protections of all products that connect to the internet.**

There are laws to protect kids' data, but not all kids are protected equally. In the United States, the Children's Online Privacy Protection Act (COPPA) regulates data collection from kids under 13 and requires parental consent before data is collected by digital platforms. However, no similar federal consent requirements exist for teens ages 13-17. Some U.S. states (like Utah, Florida, Texas, Oregon, Maryland, and California) have passed their own data privacy laws. These laws vary, but some allow you to delete personal information held by companies or limit how minors' information is sold or shared.

*The Popular Family Safety App Life360 is Selling Precise Location Data on its Tens of Millions of Users, by Jon Keegan and Alfred Ng, 2021

**Romantic AI Chatbots Don't Have Your Privacy at Heart, by Jen Caltrider, Misha Rykov, and Zoë MacDonald, Mozilla Foundation, 2024

What to notice

When personal details show up in recommendations. If ads or suggestions online start to reflect information or personal interests your kid has shared with a chatbot, it may mean their information is being sold to businesses.

If AI tools encourage kids to share their emotions. If a tool frequently asks kids questions or prompts them to share their feelings or personal experiences, it may be collecting especially sensitive information.

What you can do: Conversations to protect kids' privacy

With your kids:

We recommend these activities for kids ages 10-14. But you know your kid best! If these are relevant to you, use them!

- **Look for privacy red flags:** The Mozilla Foundation's Your Kids Tech Privacy Cheat Sheet is a good resource to help you get started. Take an extra-close look at the privacy policy of any product that records, listens to, tracks, or collects input from your kid, including chatbots, tablets, smart speakers, smartwatches, fitness trackers, and location trackers. Often, there are alternative options that collect less data and share far less (or none!) with third parties.
- **Explore privacy settings with your kid:** With your kid, open up the settings of any AI tool that they use. Explore the different options and turn on or off settings to help protect kids' privacy. Though each tool has different privacy settings, these might include:
  - Turning off the option to allow your kids' data to be used to train AI models (this is sometimes labeled as "help improve our model").
  - Turning off the option to allow your kids' past chats and memories to be used to customize the ads they see.
  - Turning off the option to allow the tool to collect and use your kids' location data.
- **Ask your kid:** Can you think of ways that companies might use your online information? What would they do with it? Brainstorm together. Offer tips if kids get stuck:
  - To send you advertisements for specific things they think you will like?
  - To convince you to spend money on products?
  - To persuade you to believe something?
  - To encourage you to look at specific links, websites, videos, or apps?
  - To keep you online and using the platform so they can keep collecting more information?
- **Remind your kid:** The things they put online are never really private. Social media and AI can track everything you say. AI chatbots can collect the most, since you talk to them directly!

In your school or community:

- If you are concerned about the privacy policies and information-sharing habits of tools using AI, learn more about how these tools are used in your school or district, stay informed about local policies, and start conversations with other families in your community.

Find more in our Parent Tip Sheet Library! For more detailed information, including data sources, check out the full report: A new direction for students in an AI world: Prosper, Prepare, Protect.

Center for Universal Education at BROOKINGS