

Apps to Watch Out For - Part 2

We use our phones for many things—to text, to call friends and family, to play games, to order food, to read articles such as this. But did you ever stop and ask yourself if the apps on your phone are actually safe to use?

If not, you probably should.

The average American has <u>40 apps</u> on his or her phone. Some of them are useful. But, according to a new report, many apps, even the ostensibly useful ones, are dangerous for your privacy. They harvest personal data and share their findings with third parties—often without our knowledge or consent.

The development of artificial intelligence (AI) has created a variety of threats to the privacy of users' data. To identify the most intrusive, data-hungry apps, researchers at Home Security Heroes <u>investigated</u> a total of 159 AI-based applications in Apple's App Store. They found the following:

- "75 percent of AI apps share users' data with third parties."
- "64 percent of investigated AI-powered apps track users' personal data for their own marketing benefits."
- Only 25 percent of the 159 apps studied refrained from sharing the data submitted to them. The other 75 percent, according to the authors of the report, "are notorious for sharing user data with third parties, including other apps, or marketing companies."
- A total of 74 percent of AI apps track identifiers, "a set of unique serial numbers or character strings that are specific to a user's device." Identifiers include user IDs, such as a screen name, handle, account ID, device ID, and so forth.
- The top six most invasive AI apps are:
 - \circ Brainly
 - Photoleap: AI Art Photo Editor
 - Google Assistant
 - Socratic by Google
 - DaVinci AI Generated Art
 - Facetune AI Photo/Video Editor

More than <u>30 million Americans</u> use Brainly, the most invasive AI-powered app on Apple's App Store, according to the report. One of the world's <u>largest online learning communities</u> for parents, students, and teachers, Brainly monitored 42.86 percent of users' personal data.

Like Brainly, Photoleap, which has been downloaded <u>millions of times</u> in the United States, monitored 42.86 percent of users' data. Close to <u>37 percent</u> of the population uses a voice assistant, and Google Assistant is the <u>most popular</u> choice. If you use Google Assistant, you might want to consider using a less data-obsessed alternative.

Protecting Kids

Apps can be harmful in ways other than harvesting data. Another <u>report</u> identified 10 apps favored by child predators to target children online, according to UK police.

These include Whisper, a social media app that allows users to post and share photos and video messages anonymously. Of the 187 countries in which Whisper is available, its biggest user base is <u>situated in the United States</u>. Pedophiles also use Calculator %. Marketed as a calculator app, it's actually a secret photo vault. Another app favored by predators is Omegle, a free online chat website that enables users to communicate with others without the need to register. Worryingly, <u>age verification</u> isn't required either.



Another app, <u>Yubo</u>, formerly known as Yellow, is best described as Tinder for teens. This app encourages youngsters to find new friends by swiping left or right. Another app on the list is Chat & Date, formerly known as Hot or Not. Like Tinder and Yubo, it promotes swiping, flirting, and real-world meetups. Hence the reason why so many child predators are so keen to use it.

If you happen to be a parent of a young, impressionable child, I would encourage you to check his or her phone to see if they've downloaded any of the apps discussed in this piece. If they have, remove them immediately. Every 24 hours, there are at least <u>half a million</u> child predators online, scouring apps and chatrooms for their next target. By faking their ages and creating a completely fabricated persona, these predators lure unsuspecting children into a false sense of security. Over a period of days, weeks, and even months, a relationship is built on a foundation of misplaced trust. Predators ask questions, take notes, then weaponize the information they gather to wall children off from their loved ones. Once isolated, the predators pounce.

The virtual world is an expansive, unruly place, full of dangerous individuals with the sickest of motives. As the line between the real world and the virtual one blurs and children spend more time online, we should expect the number of child predators to grow. Beware. Protect yourself and protect your children.

Source <u>www.EpochTimes.com</u> (John Mac Ghlionn, June 30, 2023)

If you need help:

- The National Human Trafficking Hotline in your cell phone: call 888-373-7888 (24 hours/day, 7 days/week, 365 days/year). www.humantraffickinghotline.org
- Text INFO or HELP to: BeFree 233733
- Call 911
- The National Runaway Switchboard: 1-800-RUNAWAY. www.1800RUNAWAY.org
- National Center for Missing & Exploited Children (NCMEC): 1-800-843-5678. www.missingkids.org
- Report suspected human trafficking to federal law enforcement by calling 1-866-347-2423.
- CHILD ABUSE HOTLINE 800-344-6000
- The following link provides a card with a brief list of common indicators of human trafficking, the difference between human smuggling and human trafficking, and a DHS reporting option: <u>https://www.dhs.gov/blue-campaign/materials/indicator-card</u>

Nonprofit organizations that work to stop human trafficking day in and day out need your help. Please consider donating to HuMannaTea For All[™] at: <u>https://thecause.org/partners/humannatea-for-all/</u>

The material and information contained in this document and/or on this website is for general informational purposes only. It is not an exhaustive or complete list of information relating to the topic or industry headlined. Please do not rely on this material or any information provided by HuMannaTea For All[™] as legal, medical, or otherwise licensed professional advice. Whilst we endeavor to share up to date and correct information, HuMannaTea For All[™] makes no representations or warranties of any kind, express or implied about the completeness, accuracy, reliability, suitability, or availability with respect to the website or the information, recommendations/suggestions, products, services, related graphics, and/or graphics contained on the website for any purpose. Any reliance you place on such material is therefore strictly at your own risk.