the Defender®
CHILDREN'S HEALTH DEFENSE NEWS & VIEWS

CENSORSHIP/SURVEILLANCE

'Authoritarian Nightmare?': Using AI Facial Recognition Technology to Verify Kids Ages

The Washington Post highlighted the growth of private firms using artificial intelligence facial recognition technology to identify users' ages. The technology is marketed to sites like TikTok as a means of preventing access to children.

by **Michael Nevradakis, Ph.D.**

AUGUST 12, 2024

606 **PAGEVIEWS** 1

The U.S. Department of Justice (DOJ) last week **sued TikTok**, accusing the platform of "flagrantly violating" the **Children's Online Privacy Protection Act** (COPPA), the **COPPA Rule** and a 2019 **decision by the Federal Trade Commission** (FTC) regarding the illegal collection of children's personal information.

The **lawsuit**, filed in federal court in California, alleges TikTok collected "extensive data" from children under 13 without parental consent, allowed users under 13 to create and maintain accounts, and failed to comply with parental requests to delete their children's accounts and personal information.

The lawsuit — the latest in a series of U.S. government actions against the platform — follows a complaint filed in 2020 by several advocacy groups, including the Electronic Privacy Information Center (EPIC), alleging **TikTok violated COPPA**.

In April, President Joe Biden signed a **bill banning TikTok in the U.S.** unless its Chinese parent company sells the social media platform's U.S. assets by January 2025.

The DOJ's announcement came on the heels of a **Washington Post report** Wednesday highlighting the growth of private firms using artificial intelligence (AI) facial recognition technology to identify users' ages. The technology is marketed to sites like TikTok as a means of preventing access to children.

According to the report, the technology — which is prone to false positives — has raised privacy concerns among parents. However, according to the Post, 19 states have passed laws requiring online age checks. However, those laws have faced legal and constitutional hurdles on censorship and free speech grounds.

Eva Galperin, director of cybersecurity for the Electronic Frontier Foundation (EFF), told **The Defender** that "out of the efforts that our legislators and the U.S. government have been making to pursue TikTok and limit its reach, this is probably the most reasonable. This is one with teeth."

Galperin noted, though, that other social media platforms have engaged in similar practices. She said:

> "The DOJ has gone after other social media companies for COPPA violations. So has the FTC … When the House decided to single out TikTok for banning, over privacy violations and other types of behavior, I thought that this was pretty outrageous, and the reason

> for that was that there was almost nothing that the House was alleging that TikTok was done that was not already being done by just about every other social media company in the U.S.
>
> "The only difference is that it was being done by a Chinese company and not a company located in Europe or the U.S."

Galperin cited an example:

> "We actually got the FTC to go and **investigate Google over its tracking of children** in Chromebooks years ago, where it turned out that Google was giving Chromebooks for free to schoolchildren, wasn't supposed to track anything they did while they were in school, but was in fact gathering that data."

Galperin said the EFF's 2015 complaint against Google led to further regulatory scrutiny of Google's practices.

According to **Tim Hinchliffe**, editor of **The Sociable**, the use of facial recognition technology by social media platforms and other websites and online services poses a significant risk to children.

Hinchliffe said:

> "The risks of AI facial recognition on children outweigh the benefits. Throughout our entire human existence, we've had people called parents to safeguard children. If a parent doesn't want their child's face collected and stored in a database, they should have the power and control to keep that technology from being used on their kids without prejudice."

Hinchliffe also warned that the widespread use of such technologies by children could result in a normalization of their use.

"AI face scanning on kids' programs teach them from an early age to accept that they don't have privacy, and it is the next step towards a digital identity-driven internet passport to eliminate all anonymity," Hinchliffe said.

TikTok built ‘back doors’ allowing young children access to its platform

According to the FTC, TikTok and its parent company, ByteDance, “allegedly were aware of the need to comply with the COPPA Rule and the 2019 consent order and knew about TikTok’s compliance failures that **put children’s data and privacy at risk**.”

But instead of complying, the complaint states that:

> “For years millions of American children under 13 have been using TikTok and Defendants have been collecting and retaining children’s personal information.”

The FTC wrote that as of 2020, TikTok used “human reviewers” to determine whether a user was under 13 years of age, but “allegedly spent an average of only five to seven seconds reviewing each account to make their determination of whether the account belonged to a child.”

The platform then allegedly continued to collect personal data from these children, “including data that enabled TikTok to target advertising to them — without notifying their parents and obtaining their consent as required by the COPPA Rule.”

According to the FTC, “back doors” were built into the TikTok platform “that allowed children to bypass the age gate aimed at screening children under 13.” This included using credentials imported from other **Big Tech** platforms, such as Google and Instagram. TikTok classified these accounts as “age unknown.”

TikTok used the data it collected “to build profiles on children,” and “shared this personal data with third parties such as Facebook and AppsFlyer.” The platform also allegedly made it difficult for parents to request that their child’s accounts be deleted, often ignoring parents’ removal requests.

Booming ‘age assurance’ industry leading to an ‘authoritarian nightmare’

According to the Washington Post, concerns over children gaining access to age-inappropriate content online have fueled "A **booming industry of AI age scanners**, aimed at children's faces," comprised of "a little-known group of companies in an experimental corner of the tech industry known as 'age assurance.'"

These age-assurance checks, which "rely on a style of **surveillance** that ranges 'from "somewhat privacy violating" to "authoritarian nightmare,"'" the Post reported, the door to privacy risks for anyone who uses the web and may "subject children — and everyone else — to a level of inspection rarely seen on the open internet."

While age assurance "could give parents a better sense of control and peace of mind," the Post reported that the collection and centralization of users' personal and biometric data may "boost the chances [it] could be hacked, leaked or misused."

The Post cited companies such as **Yoti**, **Incode** and **VerifyMyAge** — describing them as "digital gatekeepers" that have developed technology that asks users to verify their age by recording a "video selfie," often while holding a government ID in front of the camera. AI tools then determine the users' age, based on biometric features.

Major social media platforms and online services, including TikTok, **Facebook**, **Instagram** and **OpenAI**, and several adult-oriented websites, now use such age-check tools, while 19 states — including Florida, Texas and Virginia — have passed or enacted laws requiring online age checks.

According to the Post, such legislation has "created a gold mine," citing the example of San Francisco age verification firm Incode, which now "internally track[s] state bills and contact[s] local officials to … 'understand where … our tech fits in.'"

Children's photos and data a 'tempting' target for hackers

The expansion of age-verification services online — and the growing number of states that have enacted online age-verification laws — have also fueled criticism and concerns, the Post noted:

> "The tools' supporters acknowledge that age checks could fuel a profound expansion in government oversight of online life. But critics argue that lawmakers hoping to shield kids could instead expose users of all ages to terrible risk, forcing them to hand over intimate details of their lives to companies that are largely unproven, unregulated and unknown."

Such concerns persist despite assurances by companies like Incode and Yoti that they delete images after a user's face is analyzed.

Galperin said the data collected by such companies is housed in "Big databases containing photos of people with their real names, their IDs, their addresses and all kinds of sensitive information — and it just sits there."

This becomes a "tempting" target for hackers, Galperin said, and also places the data at risk of a breach or leak.

"This is also information that potentially becomes public, not just because of hackers but because companies make mistakes and this information ends up spilling online," she said.

Comparing centralized databases of children's biometric information to "legalized pedophilia," California-based privacy attorney **Greg Glaser** told The Defender that such data, which may potentially include "full and partial body shots of children" in private settings, would be at risk of being leaked "onto the dark web."

"At this point in history, it is obvious that computer systems are not designed with checks and balances to respect traditional morality, like the sanctity of an innocent childhood," Glaser said.

Hinchliffe said individual users' data may also be compiled and put them at risk of profiling, as "the databases would maintain a complete record of every child's stages of life." He added:

> "Researchers say that AI can already **detect sexuality** from a single photograph. Imagine what inferences they'll be able to make about children who are scanned throughout their entire lifetime. Will AI face-scanning be able to distinguish a liberal from a conservative? Can AI make inferences about a person from the way they dress, the color of their hair, their ethnicity, their microexpressions, or their tattoos?"

Galperin also warned that domestic abusers and stalkers could take advantage of leaked data from age assurance databases.

"One of the most common kidnapping scenarios in the U.S. is usually the kidnapping of a child when the parents have divorced but only one parent has been granted custody, and the parent without custody essentially takes the child," Galperin said. "This technology could potentially put people in some real danger."

"When adults experience firsthand how AI facial recognition can be used against them, I think they'd be more hesitant to allow that same technology to be used on their children. But if the technology is used on kids first, would parents realize the full extent of how dystopian it could get?"

Government and private actors may also take advantage of such data. Galperin said:

> "This data could also be tempting to advertisers and data brokers, who love this kind of info for the purposes of targeted advertising. It's also of interest to governments and law enforcement, who regularly buy data from data brokers in order to save themselves the trouble of having to go to court to get a warrant or a subpoena for certain kinds of data."

Others have argued that age assurance technology, despite the promise of AI, often results in false positives that may shut legal users out of online services.

The Post cited data from the National Institute of Standards and Technology that **age estimators** are "typically accurate within about three years," and from Instagram, finding that age checks had stopped 96% of teens who tried to change their accounts to appear over the age of 18.

But this still shuts out many potentially legitimate users, with certain groups being particularly at risk. The Post noted that the systems' error rates for girls and women were higher than for boys and men and that people with certain disabilities affecting their appearance are often shut out.

"If your solution has any kind of false positive, you're essentially locking people out of the internet who should not be locked out. Any solution that has false positives like this is unacceptable," Galperin said.

When Yoti asked the FTC last year to approve age estimators as a means of **obtaining parental consent**, more than **300 comments filed** during the public commenting period opposed the proposal, the Post reported. The FTC ultimately **denied Yoti's proposal**.