# Think FaceApp Is Scary? Wait Till You Hear About Facebook

*Author: Brian BarrettBrian Barrett*

*Gavriil Grigorov/TASS/Getty Images*

FaceApp is a viral lark that takes a convincing guess at what you'll look like when you're old. FaceApp is also the product of a Russian company that sends photos from your device to its servers, retains rights to use them in perpetuity, and performs artificial intelligence black magic on them. And so the FaceApp backlash has kicked into gear, with anxious stories and tweets warning you off of its charms. Which, fine! Just make sure you save some of that ire for bigger targets.

The response to FaceApp is predictable, if only because this cycle has happened before. FaceApp went viral when it launched in 2017, and prompted a similar—if far more muted—privacy kerfuffle. But compared to Meitu, that year's other viral face manipulator, which is quite a phrase to type, FaceApp was downright saintly in its data collection. At least FaceApp didn't access your GPS and SIM card information. More energy was directed at bigger problems, like FaceApp's blackface filter. (Yep!)

> "This is definitely not a unique FaceApp problem. FaceApp is part of a larger privacy problem."

Christine Bannan, EPIC

The latest frenzy appears to have been kicked off by a since-deleted tweet that claimed FaceApp

uploads all of your photos to the cloud. That certainly would be alarming. But FaceApp has denied the claim, and multiple security researchers have confirmed that it's not so. FaceApp takes only the photo you ask it to manipulate. The company also says it deletes "most images" from its servers within 48 hours of uploading, although admittedly there's no way to confirm that it does so in practice. If you want FaceApp to remove all of your data from its servers, you can send a request within the app, by going to **Settings > Support > Report a bug** and putting "Privacy" in the subject line. "Our support team is currently overloaded, but these requests have our priority," FaceApp founder Yaroslav Goncharov said in a statement. "We are working on the better UI for that."

Those measures don't make FaceApp some paragon of data privacy. While the way it manages photos is kosher under Apple rules, FaceApp doesn't make it clear enough to users that it's sending them to a server. "I cannot think of any situation where an app should not be very painfully clear about a photo being uploaded to a remote server," says Will Strafach, security researcher and developer of Guardian, an iOS firewall app. "Users always have the right to know this."

Still, it's important to note that while FaceApp calls St. Petersburg home, its servers are based in the US. The company said in a statement that "the user data is not transferred to Russia." Like almost everyone else, FaceApp uses Amazon's cloud. And it has at least a plausible reason for doing so: The processing power required to apply a Methuselahn filter on your face is more manageable there than on your device. More recent iPhones and Android devices have machine learning capabilities baked into their hardware, but it's safe to assume that plenty of FaceApp's reported 80 million users are on older models.

So what's changed since 2017? On the FaceApp side, not much. But the world around it looks markedly different. Russia has become synonymous with nefarious online meddling, to the point that any company—even a silly filter app—becomes a bogeyman. Awareness of facial recognition's perils has reached something close to critical mass. And the idea that one's personal data might be worth protecting has gained real, immutable traction.

All for the better, or at least on those last two points. You *should* ask questions about FaceApp. You should be extremely cautious about what data you choose to share with it, especially something as personal as a photo of your face. But the idea that FaceApp is somehow exceptionally dangerous threatens to obscure the real point: All apps deserve this level of scrutiny—including, and especially, the ones you use the most.

"People give photos to lots of different apps. I think this is probably getting attention because it's Russian developers," says Christine Bannan, consumer protection counsel at the nonprofit Electronic Privacy Information Center. "But this is definitely not a unique FaceApp problem. FaceApp is part of a larger privacy problem."

Take the most obvious example, and not only for its similar name. Facebook has nearly 2.5 billion monthly active users to FaceApp's 80 million. It, too, applies facial recognition to photos that those users upload to its servers. It also actively pushed a VPN that allowed it to track the activity of anyone who installed it not just within the Facebook app but anywhere on their phone. When Apple finally banned that app, Facebook snuck it in again through the backdoor. And that's before you get to the privacy violations that have led to a reported $5 billion fine from the FTC, a record by orders of magnitude.

People have expressed concern that FaceApp's terms of service includes "a perpetual, irrevocable, nonexclusive, royalty-free, worldwide, fully-paid, transferable sub-licensable license to use, reproduce, modify, adapt, publish, translate, create derivative works from, distribute, publicly perform and display your User Content and any name, username or likeness provided in connection with your User Content in all media formats and channels now known or later developed, without compensation to you." Rightly so. But see how closely it mirrors Facebook's terms of service, which also says that "when you share, post, or upload content that is covered by intellectual property rights (like photos or videos) on or in connection with our Products, you grant us a non-exclusive, transferable, sub-licensable, royalty-free, and worldwide license to host, use, distribute, modify, run, copy, publicly perform or display, translate,

and create derivative works of your content (consistent with your privacy and application settings)." (Which is as good a reminder as any to lock down your Facebook privacy settings.)

And it's obviously not just Facebook. Look at Life360, a family-tracking app that turns user data into revenue through advertising and partnerships. TikTok is based in China, a country with a damning history of facial recognition abuses. For years, US carriers sold detailed location data of their customers without explicit consent. As noted by *Ad Week* reporter Shoshana Wodinsky, FaceApp itself sends data to DoubleClick, the Google-owned ad company, and to Facebook. And so do countless others.

Should you be worried about FaceApp? Sure. But not necessarily more than any other app you let into your photo library. Or any other part of your phone.

"I wish people would think before they try out any app, but that just isn't realistic. People want to use cool-looking services and they'll never read a boring privacy policy before doing so," says Joseph Jerome, privacy counsel at the nonprofit Center for Democracy & Technology. "There's a real tension between individuals wanting to have fun with their photos and their images being used for a host of different facial recognition and image analytics products. This is why we've been calling for regulations around biometric data."

Instead of these panics, which fade in and out in step with the virality of their targets, maybe a healthier focus is on broader awareness. Your data has value. Think twice about who you give it to, regardless of what country they're in or how silly they make you look.

---

## More Great WIRED Stories

- The cryptocurrency rush transforming old Swiss mines
- The death of a patient and the future of fecal transplants
- Explaining the "gender data gap," from phones to transit
- One boy's dream vacation to see construction equipment
- Inside Backpage.com's vicious battle with the Feds
- 🎧 Things not sounding right? Check out our favorite wireless headphones, soundbars, and bluetooth speakers
- ✉️ Want more? Sign up for our daily newsletter and never miss our latest and greatest stories