

FaceApp: Photoshopping on Steroids

By Dean Nicolls | July 19, 2019



Check out the [before and after pictures](#) The Jonas Brothers created with FaceApp. While the app has been around since 2017, it's gone viral in the last week as people use it to see how they would look when they're older.

Pretty cool. Pretty innocuous. Well, maybe, not so much.

Let's start with FaceApp's own [terms of service](#). Section 5 "grants FaceApp 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."

While this is certainly troubling, there's potentially a bigger concern. [Deepfakes](#).

When you use FaceApp, you're sending them high-res pictures of yourself as well as your name which can easily be combined with other third-party data sources to identify the personal details of the app user. The emergence of deepfake technology and computational learning models make FaceApp a legitimate security threat (which is somewhat heightened given the company's Russian roots). These sophisticated models can create deepfakes from a single or just a few images. So, now FaceApp has the capability to create high-fidelity images that are indistinguishable from the genuine article if criminally motivated.

If these images and data fell into the wrong hands, bad actors have the ability to impersonate just about anyone. This poses an obvious threat to any organization that onboards new customers and wants to ensure that someone is who they claim to be. While many online identity verification solutions require users to provide a copy of government-issued ID and a selfie, this is clearly insufficient in the wake of the deepfake threat.

That's why certified liveness detection is now so crucial.

With liveness detection, new and returning users need to effectively prove that they are physically present to guard against fraudulent attempts to gain access to personal data or use a stolen identity. Unfortunately, biometric authentication is susceptible to presentation attacks such as spoofing, that attempt to bypass biometric identity verification. Fraudsters will often try to spoof the system using a doctored photo, screen image, a recording or doctored video — all of which can now be made even more lifelike with deepfake technology.

With liveness detection, the online user is prompted to perform an action that cannot be easily replicated with a spoof. It might involve keystroke analysis, recording a series of random numbers, eyeball tracking or flashing lights on the user's face. At Jumio, we've embedded FaceTec's patented ZoOm technology into our identity verification and authentication workflows. Using this technology, users just fit their face into a small oval on the screen, and the oval gets larger and the user move closer to fit into the second oval. During the two-second process, we capture 30-60 frames of video per second and create an encrypted 3D face map, in which perspective distortion, or the fisheye effect, is measured. If it's not a three-dimensional object, FaceTec's algorithms will conclude it's a 2D image like a picture, rejecting the spoof attempt.

In other words, liveness detection is your secret weapon against deepfakes.

If you can prove liveness, particularly during enrollment, that establishes the chain of trust. It anchors the digital identity of a real person and strengthens the entire trust chain, especially if the biometric data is stored centrally.

Liveness detection coupled with 3D face matching is an effective way of stopping the majority of account takeover attempts. Just like any company should take a "trust but verify" approach to onboarding new customers, they need to do the same with their verification providers, especially when it comes to validating unsubstantiated performance claims about their ability to spot spoofs and deepfakes.