The FaceApp Controversy Is a Reminder of How Ill-Equipped We Are for the Surveillance of the Future

John Loeffler

Unless you've been locked in a dungeon this week, you've seen the explosion of photos of your friends, celebrities, or other online personalities you follow looking all wrinkled and gray, all generated by the mobile app FaceApp. This isn't FaceApp's first viral moment, it went viral once before in 2017, but 2017 wasn't 2019.

The rumblings over Cambridge Analytica had not yet become the privacy earthquake that would begin the obliteration of trust in Facebook and others over the intervening two years, so FaceApp could be passed off as harmless fun, no need to read the Terms of Service. Now, our understanding of the threats to our privacy has grown and while FaceApp might still be totally harmless, whether it is or not hasn't been the problem for some time. The problem, fundamentally, is us.

The Controversy Over FaceApp Explained

It has been about a week since FaceApp caught fire for the second time--they were called out for being super-problematic the first time around too--and we've already gone from the initial FOMO to the social media hangover--and in many cases, there are feelings of shame for having been caught up in what appears to be a genuine privacy violation.

RELATED: FACEAPP GOES VIRAL WITH CELEBRITIES POSTING IMAGES OF FUTURE OLDER SELVES

By now, you know exactly what we're talking about here: the first half of the week, everybody you knew on social media was snapping selfies and uploading what FaceApp's AI's best guess as to how they'd look as old people.

> When you take a trip to the Year 3000. pic.twitter.com/O9Dxpwj6ex
>
> — Jonas Brothers (@jonasbrothers) July 16, 2019

> Me hosting #MasterChef Season 50.....#faceapp pic.twitter.com/uKnfxUpC1D
>
> — Gordon Ramsay (@GordonRamsay) July 16, 2019

Around Wednesday, people started pointing out that FaceApp users had all just given some company they didn't know the pertetual right to use their image for whatever purpose they want. It was all a cunning data-harvesting operation that we were all falling for.

> I thought we agreed a while back that the FaceApp was hella shady and probably using people's photos to develop facial recognition technology that will ultimately serve the surveillance state? Nothing fun is free on these social media streets.
>
> — Saeed Jones (@theferocity) July 16, 2019

> I'm glad y'all are having fun with that face-aging app but I will never be able to shake the feeling that allllllll those pics are being put straight into some kind of database, the sinister purpose of which won't be revealed until it's too late.

> — Scott Wampler™ (@ScottWamplerBMD) July 16, 2019

> I can't but help to think this FaceApp is collecting our data for something shady. But I want to try it
>
> — Cornelius (@koolexposure) July 16, 2019

Privacy advocates and politicians started raising concerns about where exactly these images were being stored, publicizing the fact that the actually processing of your image wasn't happening on your phone, but on cloud servers somewhere else. Then came the 'revelation' that FaceApp was headquartered in--cue ominous music--St. Petersburg, Russia.

> HOWEVER: they do appear to upload single images in order to apply the filters server-side. while not as egregious, this is non-obvious and I am sure many folks are not cool with that.
>
> — Will Strafach (@chronic) July 17, 2019

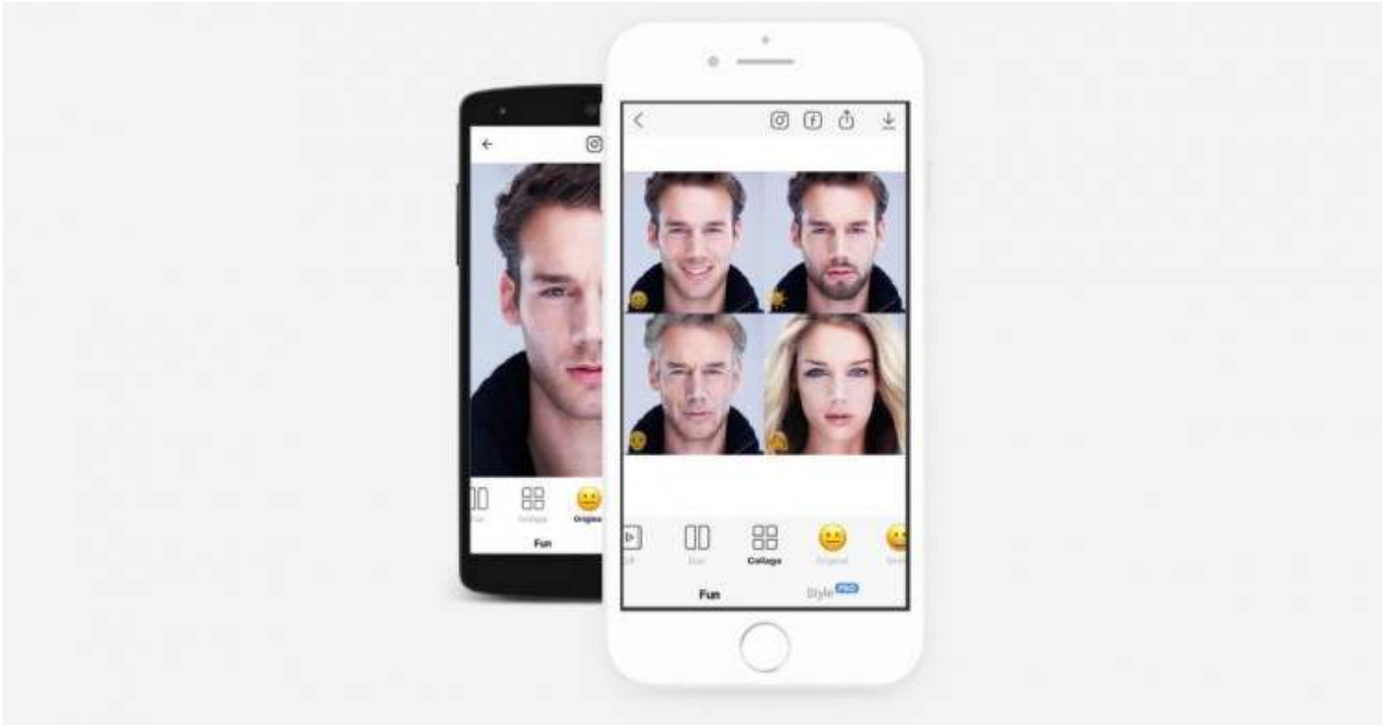
> Their Privacy Policy is not remotely GDPR compliant. It says that your data can be transferred to any location where they have a facility ... which means Russia.
>
> — Elizabeth Potts Weinstein (@ElizabethPW) July 17, 2019

> BIG: Share if you used #FaceApp:
>
> The @FBI & @FTC must look into the national security & privacy risks now
>
> Because millions of Americans have used it
>
> It's owned by a Russia-based company
>
> And users are required to provide full, irrevocable access to their personal photos & data pic.twitter.com/cejLLwBQcr
>
> — Chuck Schumer (@SenSchumer) July 18, 2019

So here we are on Friday and the tone of the conversation has shifted 180 degrees from 'Hey! This is cool!' to 'Oh no, what did we all just do?' in about 100 hours. We want people to think that we're all smarter than this, but a lot of people may be feeling sheepish about it, especially when half the internet is calling all the FaceApp users easy marks for a Russian intelligence operative.

But is it really that serious?

Should You Be Concerned About FaceApp?

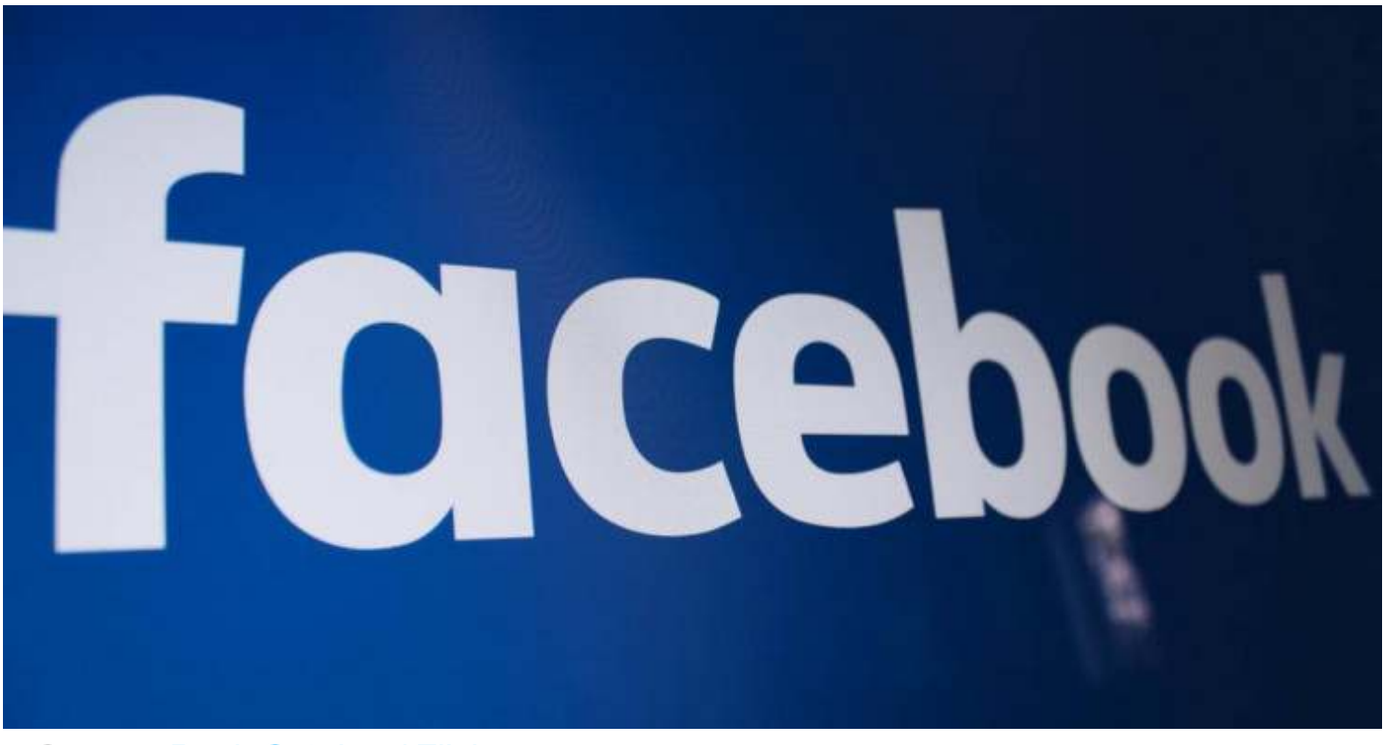


Source: FaceApp

This scenario has been playing itself out with dozens of viral trends over the past few years that involved uploading your image to something. Last year, we went through this exact controversy over the whole 'find a historic work of art that looks like you' Google app, minus the Red Scare element to it. Likewise Facebook's '10-Year Challenge'.

There is some genuine concern here, obviously. It has always been the case that whenever someone is offering you something for free, what they're after is the information you need to provide in order to get that free thing. This is how mailing lists have been built up for more than a century.

Similarly, the whole concept of television ratings is built on gathering data from so-called Nielsen families; those households that allow the Nielsen company to monitor what shows people are watching or radio stations they are listening to so networks can set a price for ad space and businesses can decide where to advertize based on the size of the audience.



Source: Book Catalog / Flickr

Is FaceApp--or Facebook or other social media and internet companies that make money mining user data--really all that different? The principles are pretty much the same, but the scope of the user data collected from Nielsen viewers and Facebook users is like the difference between the multiplying a number by 10 and raising a number by 10.

You can tell what a Nielsen household is watching, but you can't really tell who is watching it, or whether they are rooting for one team or the other during the Superbowl. Also, at least traditionally, Neilsen has been up front about the purpose their data collection serves and Neilsen families went in understanding exactly what information they are giving up in the process. They could also drop out of the program and the data would stop being collected.

Facebook has built an entire profile of a user based off data collected even outside of Facebook itself. This is then used to micro-target advertising and content delivery with such specificity, and does so without supervision, that these profiles become problematic. If someone is pregnant, lets say, and they want to keep that information private but they search for OBGYNs or click on a pregnancy resource center's Facebook page, Facebook may determine that a user is pregnant and start pushing ads featuring baby products to that person.

While Facebook might have specific safeguards around that kind of profile building, we know they weren't always so careful about the way their data was being used to target users. Facebook famously got itself into trouble for giving advertisers the option a few years ago of targeting their advertising along ethnic and racial lines by excluding certain groups or categories with strong racial, ethnic, or religious associations. These exclusions could allow advertisers to discriminate against these groups for products and services such as housing or employment.

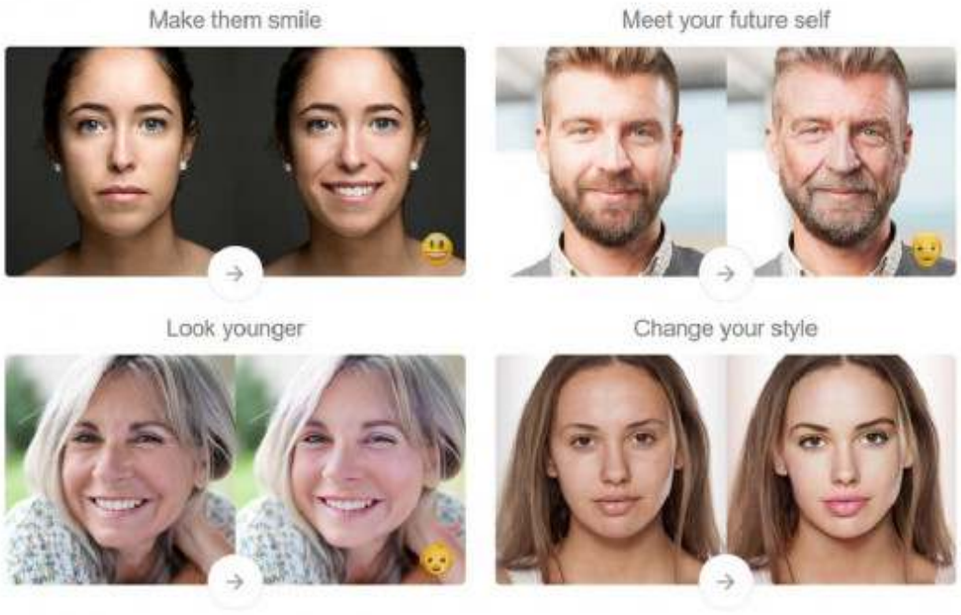
Facebook removed over 5,000 target categories for their ads based off these concerns. As bad as that is, they were only able to build those categories in the first place by reversed-engineering the likely ethnicity, race, or religious beliefs of a user based on the user's activity, which isn't simply offensive but outright dangerous in a world where these categories have often been used as a basis for oppression and far worse.

While its doubtful that Facebook is collecting data to build those profiles in order to oppress ethnic, religious, or racial minorities, the same can't be said of China, who is currently running concentration camps for over a million Muslim-majority Uighers in that country for the purpose of 'deradicalization'.

Data collection has been a major part of that effort. The data gathered from their cell phones, public interactions, and sometimes simply seized by police though forced biometric recording at police stations has been used to create de facto house arrests as AI systems and facial recognition sensors alert police whenever someone identified as Uigher enters certain public spaces, such as hospitals.

If you think that your data isn't that big a deal, the current plight of the Uighers should dispel any notion that your data can't be used against you.

The Problem Isn't FaceApp



Source: FaceApp

The problem is not that FaceApp is going to use the image of our faces for something other than entertaining us by turning all of us and our friends into a bunch of Olds. And, despite the claims of a lot of people online and some politicians here in the US, there is no evidence that anyone has turned up that FaceApp is uploading your camera rolls to their cloud servers.

What they're almost certainly using your image for is some kind of training data for the kind of generative-AI that produces deep fakes and the like. If that's the case, then you have absolutely nothing to worry about. Once that data has been processed by the AI system they want to train, it will likely be thrown out since it's pretty much useless after that.

The company CEO has reportedly said that people's images are typically deleted after a short time--though to be clear, he has said nothing about what those images are being used for by the company beyond training their neural network.

Much has been made of the company's privacy policy which reserves the right to use your image for any legitimate business purpose, which could include using them in product advertizing. They also promise not to sell your data to third-parties, but reserve the right to share your data with any affiliate companies. So anyone who buys FaceApp could get access to whatever data they have on you.

Both of which are highly problematic, but honestly that's because this is pretty much boilerplate legalese for businesses that rely in some way on data-mining. A lot is being said about how Facebook is worse than FaceApp, and they certainly are, but this problem is even bigger than Facebook.

The issue that privacy advocates have is with the regulatory Thunderdome we're living in which pits hapless users with no legal training into a battle of language with skilled lawyers whose entire job is to exhaust the user into just saying 'Eff it' and clicking the accept button.

The fact that--after we find out through the media or word of mouth, like normal people in other words, what was actually in those terms of service--it is an entirely acceptable defense for the company to say 'Well, you agreed to it by clicking accept' is the fundamental problem, and there's no simple fix to that. It is a political problem, not a legal one. This tactic has been used by companies to get us to surrender our rights to everything from our images and videos to our right to sue a company for discrimination.

And let's also be clear that the problem isn't that the company is Russian. Based in St. Petersburg, FaceApp's viral moment has brought out all kinds of almost McCarthyite-levels of paranoia. The

Democratic Party freaked out this week and instructed everyone working on the campaigns to delete FaceApp from their phones immediately.

Granted, I get why they're a bit touchy about this, but after 2016, why the hell do any of you *any* data collecting apps on your phones? They all collect data and can all be used to gain unauthorized access. FaceApp might be some kind of sinister Russian intelligence operation to collect the faces of Americans to help re-elect Donald Trump or something, but if someone could draw that line from one thing to the other, I'd love to see it.

The Backlash Against FaceApp Isn't About FaceApp Either

Our looking for people or nefarious governments to blame does speak to a larger anxiety that is actually a symptom of what is really problematic about FaceApp. You don't need lines of evidence when you've been victimized in the past by a scheme that to this day is still difficult to understand. Not that it didn't *happen* but that its really hard to understand for most people.

Cambridge Analytica *did* scrape tens of millions of Facebook users' data to help target electioneering efforts, but do you know how they did it, or what that even means? The Russian Intelligence services *did* engage in a coordinated misinformation campaign to disrupt the 2016 US Presidential election and may have run similar campaigns in Europe over the last few years, but with so many moving parts and with many of the details still locked up behind ongoing investigations, the conspiracies have taken over in the absence of fact.

And while we're at it, the CIA definitely engaged in these kinds of campaigns around the world during the Cold War and likely still does to this day. China doesn't even hide the fact that is weaponizing the data it is collecting on its citizens to implement a system of social and behavioral control that insulates the state against dissenters.

But unlike past propaganda efforts, most people realize that they are way out of their element when it comes to the technology involved. If you aren't versed in deep fakes, AI, and the way information propagates through a social network, its hard to connect the sense of feeling duped to the people who conned you. When you have no one to charge with the offense, then everyone and everything becomes suspect.

And this is not paranoia, honestly. Governments and large institutions of all kinds have used the collection and control of information as a way to acheive and maintain power for as long as there have been governments and institutions of any size whatsoever. What makes our current situation so distressing for people is that we're all waking up to the fact that as savvy as we all thought we were, we're as easily manipulated as our rustic, country ancestors who lived and died firmly believing that their ruler lorded over them by divine right and that this was just.

The problem isn't FaceApp or that we all fell for some kind of scary Russian plot; the problem is that we really don't seem capable of distinguishing one from the other, either before or after the fact. Throw in a little FOMO and a couple of paid-celebrity endorsements and we will give the app or quiz or product whatever they want from us--even our faces, the most personal identifying information there is--and only revisit that decision once others start pointing out that this could be dangerous.

The real concern with FaceApp is that it shows just how unprepared we all are for the level of surveillance and data-collection that is coming. If we can't muster just an ounce of skepticism for FaceApp, what exactly will make us stop and reconsider what we are sharing? Technology isn't going to get worse at collecting our data in the coming years, its going to get exponentially better at digging into our lives and pulling out all sorts of stuff we'd like to keep to ourselves. We need to find ways to at least make them work for it.

If we can give a selfie to a strange app whose privacy policy and terms of service very, very few of us read beforehand, we have very little hope that we'll be able to resist the next viral trend designed to get

us to let down our guard for some underlying data-mining purpose. We have to get better at resisting the pull to surrender our data, sure, but we also have to regulate these companies and the way we are manipulated into agreeing to things we wouldn't is we were fully informed.

Companies depend on our going along with their terms of service by making them inpenetrable. They shouldn't be allowed to do so because next time, it may not by something as benign as training FaceApp's AI; it could be much, much more sinister and we won't be able to recognize that before surrendering our most intimate details to whoever is on the other side of the cloud.