The New York Times

FaceApp Shows We Care About Privacy but Don't Understand It

There are good lessons to learn from an overblown controversy.

By Charlie Warzel
Mr. Warzel is an Opinion writer at large.

July 18, 2019

FaceApp, a mobile face-editing application, has all the necessary components for a viral privacy scandal: a catchy concept, celebrity users, a mysterious company and a stampede of public interest.

Here's the rundown of FaceApp's 15 minutes of fame: A viral app lets us see what we might look like as a wrinkle-laden 75-year-old. Users click "yes" on the terms of service without looking, and start snapping and uploading pictures.

Inevitably, just as the app reaches cultural saturation (LeBron James is doing it!), the privacy advocates, scolds and even the conspiracy theorists come out to play buzzkill.

Did you read the privacy policy? Do you know what you're giving away? How much do you know about this company — did you know they're based in Russia?

Excitement quickly turns to shame, and then outrage — we've been duped! There's overreaction. The Democratic National Committee sends out a panicked warning telling staffers and campaigns to delete it.

Then, there's a backlash to the outrage. Is FaceApp really any worse than Facebook or any other American tech company? Doesn't the United States government have a massive digital surveillance apparatus? Is this entire controversy a red scare?

[If you're online — and you are — chances are someone is using your information. We'll tell you what you can do about it. Sign up for our limited-run newsletter.]

The truth is somewhere in the middle. The FaceApp controversy seems largely overblown. No, it's probably not a Russian intelligence operation intended to steal your face in order to train deep neural networks to build elegant, democracy destroying deepfake videos. FaceApp's C.E.O. said that the company's servers are not based in Russia and claims no user data is sent there. It's supposedly not running our photos into facial recognition databases. Nor does FaceApp "sell or share any user data with any third parties," according to its C.E.O.

Yet FaceApp's privacy policy is, as many pointed out, pretty awful. It asks for "irrevocable, nonexclusive, royalty-free, worldwide, fully paid, transferable sub-licensable license" for those pictures of our faces. Despite not "selling or sharing" user data with third parties, a Washington Post columnist found third-party trackers for Facebook and AdMob embedded in the app. The app also didn't make clear to users that their images were being processed in the cloud, not locally.

And, of course, the data we're sending away, to a company that was once in trouble for creating a photo filter some users called racist, is highly personal. Deleting the app doesn't guarantee that your photos are removed from the cloud. And when FaceApp's C.E.O. says the company deletes "most" of the photos off its servers in 48 hours we have only his word to go on.

Privacy professionals and journalists have rightly noted that the real scandal here isn't that FaceApp is an outlier, but approaching the industry standard. The vast majority of apps we download have bloated, hard-to-read privacy policies. They're written by teams of highly paid lawyers looking to grant as many permissions as possible to the companies at the expense of the users. Once installed, apps are quietly sending sensitive user data (location, photos, microphone and gyroscope information) to ad networks, data brokers and other massive technology companies.

Not only are users unaware, there's almost no good way to monitor this happening or to know where all that information eventually ends up. And it's not just apps. Our biggest tech platforms and the tools they build all run off the personal data we shed.

Whether it's the countless, massive data breaches or politically-focused scandals like Cambridge Analytica, we're beginning to understand technology companies less as gadget makers and magicians and more as powerful monoliths who've stripped us of agency and control. A broad privacy reckoning is underway, though we're still in the earliest days.

But these reckonings don't just happen. They require a spark. Cambridge Analytica, which remarkably connected Steve Bannon, the Mercer family, Facebook, psychographic profiling and the 2016 Trump campaign, was such a spark. To date, it's still unclear exactly what role

psychographic profiling or Cambridge Analytica played in the 2016 election, if any. And, like FaceApp's scandal, portions of the outrage may have been misdirected, overblown or incompletely reported.

What's important about Cambridge Analytica is that it was not merely outrage from professionals, but a true cultural moment that forces us to collectively reconsider the potential implications of the technology we've built. Even though we absolutely shouldn't equate this week's FaceApp scandal with Cambridge Analytica in terms of importance or scale, FaceApp's viral rise and fallout is also a mainstream cultural moment that has people thinking critically about their apps, the terms of service they agree to and their privacy.

Yes, it's been messy and there's been unnecessary panic and finger-pointing, because we care about our digital privacy but still don't quite understand it. Which is what makes the last week potentially heartening in the long term. Privacy is complex and often dull and hard to get even concerned internet dwellers to pay attention to. This week, however, we're paying attention. We're pausing, if only for a moment, to think about the companies behind the apps we download. Another step toward a much needed reckoning.

Like other media companies, The Times collects data on its visitors when they read stories like this one. For more detail please see our privacy policy and our publisher's description of The Times's practices and continued steps to increase transparency and protections.

Follow @privacyproject on Twitter and The New York Times Opinion Section on Facebook and Instagram.

Charlie Warzel, a New York Times Opinion writer at large, covers technology, media, politics and online extremism. He welcomes your tips and feedback: charlie.warzel@nytimes.com | @cwarzel