FaceApp and Privacy Concerns: We Did it to Ourselves

techimage.com/blog/faceapp-privacy-concerns

By Mary Beth Nevulis July 19, 2019

If you woke up last week to a Facebook or Twitter feed full of your friends' faces with a new set of wrinkles and gray hair, you're not alone.

FaceApp is an iPhone and Android app that digitally alters your photos, using filters, to make you look older or younger, or a different gender, or give you bangs or facial hair. The "old age" filter has gone viral recently because it's free within the app, and this was followed swiftly by an outcry of privacy concerns and questions about how the data the app collects – including your face – is being or will be used.

The privacy policy indicates it pulls info like your location, IP address and log file information so it can target ads to you – nothing new, of course, as companies like Amazon and Facebook do the same thing for the same reasons.

But the app also needs access to the photos on your phone to work. This means, in theory, the app developers could use the app to pull all of your photos onto their servers for some kind of future use, and/or pass your photos to other organizations – and by agreeing to their terms of service, you've given them the green light.

FaceApp's terms of service include the following language: "You grant 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."

Sounds a little unsettling, right? Well, as Wired put it, "Think FaceApp is scary? Wait until you hear about Facebook." It's not just FaceApp that has the potential to use and abuse your data – it's any app or website you allow to collect and your information.

You don't need to be wearing a tinfoil hat to be concerned – but the mistake many of us are guilty of making is that we've waited too long to worry. Most people understand that they have to sacrifice a bit of privacy to maximize the ways we use apps and websites, but the extent to which we've given up our rights has only recently drawn attention, with scandals like Cambridge Analytica and confirmation that Russian intelligence used social media in order to spread propaganda during the 2016 U.S. presidential election.

Senate Minority Leader Chuck Schumer is calling for an investigation into FaceApp. This could be a positive sign that regulatory bodies will start cracking down on app developers and software companies to more fully disclose what happens to users' data – but until that happens, we need to shoulder some responsibility.

As controversies brew around facial recognition technology and deepfakes keep getting better, it's important to remember that seeing isn't always believing, and Internet giants not being evil is a thing of the past. Take steps to educate yourself on what rights you sign away when you use certain apps or technologies – and instead of wondering what you might look like in 30 years, wonder where your data might eventually end up.