# FACEAPP AND ITS TARGETED AUDIENCE

[*NB: Please check the byline, thanks! /~Rayne*]

You may have seen the buzz earlier this week across social media when cellphone users loaded and used a mobile app which applied an aging filter to a selfie photo so users could see a predictive image of their future face.

Except the vain and foolish downloaded an app developed in Russia – an app with the most ridiculous terms of service. More at this Twitter thread by @PrivacyMatters:

> If you are thinking of using the #FaceApp consider Section 5 of the ToS & that you grant FaceApp a perpetual, irrevocable, nonexclusive, royalty-free, worldwide, fully-paid, transferable sub-licensable licence to use your content (and which may be of your friends or colleagues)
>
> — Privacy Matters (@PrivacyMatters) July 17, 2019

The app doesn't make it easy to find their Terms of Service (TOS) or Privacy Policy, which to me is a red flag.

Russia does not fall under the EU's Global Data Privacy Regulation, meaning users cannot have expectations of privacy and government oversight protecting their data. Russia ratified the Council of Europe's Data Protection Convention 108 in 2013 but this appears to be little more than a head fake when Russians have taken Facebook data and used it for adverse micro-targeting against U.S. citizens in 2016. If the convention had been taken seriously, Russia's government would also have investigated the Internet Research Agency for abusing personal data without users' consent after the Department of Justice indicted IRA members.

The app's developers say users' data isn't hosted in Russia, clarifying after initial inquiries that only a limited amount of each users' data was hosted on Amazon Web Services and Google Cloud — but how would the average user be able to validate this claim? The question of hosting seems at odds with the developers' explanation that

The Democratic National Committee issued a warning to 2020 campaigns that FaceApp should not be used and should be removed from devices.

It's ridiculous that after the DNC was hacked and state election systems breached or targeted by Russia in 2016 that any sentient Democrat working or volunteering for a Democratic candidate's campaign would be stupid enough to download and use this app, if they even read the TOS. But the  viral popularity of the application and the platforms on which its output was most often shared likely propelled its dispersion even among those who should know better.

Which brings up the app's targeted audience: younger people who share images frequently in social media.

The app required users' social media identity; it captured the IMEI address of the device they were using. Imagine being able to TREASUREMAP all these users over the internet and LANs.

Finally, the app captured the users' image for editing. Imagine this data linked to all of a user's Facebook data, matched to their DMV records including their photo, validated by phone number if recorded by DMV.

It'd be insanely easy to 'clone' these users in both content and in photos and in videos using Deep Fake technology.

It'd be a snap to micro-target them for political messaging and to make threats using manufactured kompromat.

All of this should be particularly worrying

since the audience for this application is the youngest voter age groups which are least likely to vote for Trump and the GOP.

And they are the largest portion of the U.S. military. Think of what the FitBit app disclosed to any snoopers watching military bases. How many users who downloaded FaceApp were active duty or their family members?

Imagine FaceApp and all the other social data, public and private, synced with their phone which reveals their physical location. These users are entirely touchable.

There've been quite a few rebuttals to those worried about FaceApp; most complain that such concerns are merely Russia-as-boogeyman fearmongering and that U.S. Big Tech and Chinese apps like TikTok are just as bad (or worse) about collecting too much personal data and misusing it without users' consent. Or they minimize the risk by theorizing the estimated 150 million selfies collected may train a Russian facial recognition app without users' consent.

Except Europeans can rely on the GDPR for recourse and Americans have recourse through U.S. laws; they can also press for changes in legislation (assuming the obstructive Senate Majority Leader pulls his thumb out of his backside and does something constructive for once).

One other concern not touched upon is that we don't know what this particular app can do over the long run even if deleted.

Researchers looking at it *now* may find it is rather inert apart from the invasive collection of personal photos.

But what about *future* updates? Can this app push malware which can collect other information from users' devices?

And what about the photos themselves, once captured and stored. Could the developers embed

detailed tracking in the images just as Facebook has?

Bottomline: FaceApp is a huge security risk. It may not be the only one but it’s one we know about now.

We need to regulate not only personal data collection but applications which collect data – their developers must be more transparent and upfront with what the app does with data before the app is downloaded.

We also need to work with Big Tech platforms through which apps like FaceApp are downloaded. We’re back to the question whether they’re publishers or utilities and what role they play in enabling dispersion of apps which can be weaponized against users.

And we may need to institute some kind of watchdog to detect risks before they reach the public. Perhaps as part of the regulation of personal data collection a licensing or clearinghouse process should be established before apps are permitted access to the marketplace. Apple has done the best job of the Big Tech so far in policing which apps are permitted in its market. Should gatekeeping for national security interests rest solely on a few corporations, though?

*This is an open thread.*