Geoffrey A. Fowler, tech columnist for the *Washington Post*, opens his July 17 **article** with a question that's pertinent to millions of app users: "When an app goes viral, how can you know whether it's all good fun — or covertly violating your privacy by, say, sending your face to the Russian government?"

In an email response, the founder of Russian-based FaceApp answers Fowler's question: Yaroslav Goncharov asserts user data is not transferred to Russia.

But should Russian servers even be our chief concern?

Fowler's article opens with a focus on that issue – including a link to an **article** describing N.Y. Sen. Charles Schumer's call for an investigation of FaceApp based on "security concerns and Russian ties" – but his *Post* piece quickly transitions into more important questions about the company's terms-of-use statement, the routine trust that consumers place in gatekeepers like Google and Apple to vet the app makers, and some of the questions consumers *should* be asking themselves about any app that uses their personal information.

In brief, FaceApp applies artificial intelligence (AI) to photos to illustrate how a person might age. Millions of users have submitted photos of their faces and those of public figures, but few submitters were probably aware of the privacy and other risks involved.

John Koetsier, writing for ***Forbes.com***, also exhibits deep concerns about the FaceApp **terms of use**, and includes an excerpt of its broad licensing 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. When you post or otherwise share User Content on or through our Services, you understand that your User Content and any associated information (such as your [username], location or profile photo) will be visible to the public."

Indeed, such language should keep privacy advocates awake at night – as well as all consumers of FaceApp and other programs. Most FaceApp users routinely click "accept" to

this language, unaware they're permitting the company to use their images in perpetuity in just about any fashion it wishes. Imagine your image in an advertisement for something you find embarrassing. There are other issues, too, including that you "warrant" that you own the images uploaded, have the right to enter into the terms, and "agree to pay for all royalties, fees, and any other monies owed by reason of the User Content you stylize…" through the app. Were those really your intentions?

Still another concern is that FaceApp accesses other information on a device. In Koetsier's July 17 *Forbes.com* article, Rob Le Gesse, former Rackspace manager, says, "To make FaceApp actually work, you have to give it permissions to access your photos – ALL of them. But it also gains access to Siri and Search."

A second *Forbes* writer, Thomas Brewster, attempts to add perspective to the FaceApp furor, in his July 17 **article** titled "FaceApp: Is The Russian Face-Aging App A Danger To Your Privacy?"

He suggests the heightened concern stems from a developer's tweet that "set off a minor internet panic." The tweet mirrors the allegation cited by Rackspace's Le Gesse – that FaceApp might be taking every photo from your phone and uploading them to its servers.

By and large, Brewster suggests that FaceApp is not unique. By clicking blindly through *any* app's terms of use, consumers are giving the programs permission to do more than they may ever realize: "Users who are (understandably) concerned about the app having permission to access any photos at all might want to look at all the tools they have on their smartphone. It's likely many have access to photos and an awful lot more."

The FaceApp situation, like those before it and those surely to come, reminds us that it remains the consumer's responsibility to read and analyze the terms of service for *any* app before clicking "accept."

Concerns Over FaceApp Remind Us That Users May Not Fathom the Permissions They Grant Apps

Geoffrey A. Fowler, tech columnist for the Washington Post, opens his July 17 article with a question that's pertinent to millions of app users: "When an app goes viral, how can you know whether it's all good fun — or covertly violating your privacy by, say, sending your face to the Russian government?"

In an email response, the founder of Russian-based FaceApp answers Fowler's question: Yaroslav Goncharov asserts user data is not transferred to Russia.

But should Russian servers even be our chief concern?

Fowler's article opens with a focus on that issue – including a link to an article describing N.Y. Sen. Charles Schumer's call for an investigation of FaceApp based on "security concerns and Russian ties" – but his Post piece quickly transitions into more important questions about the company's terms-of-use statement, the routine trust that consumers place in gatekeepers like Google and Apple to vet the app makers, and some of the questions consumers should be asking themselves about any app that uses their personal information.

In brief, FaceApp applies artificial intelligence (AI) to photos to illustrate how a person might age. Millions of users have submitted photos of their faces and those of public figures, but

View the **PDF version** of this article.
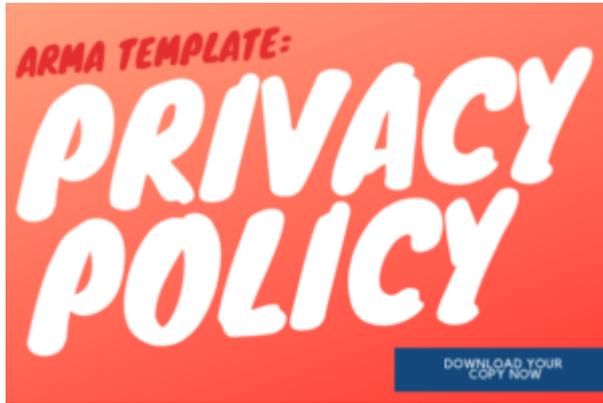
Privacy Policy Template

Originally developed by Jim Koziol, this Privacy Policy Template will help you establish a privacy policy at your organization or give you some ideas on how to enhance your existing privacy policy.

Download

Author

- ARMA International

(Visited 641 times, 1 visits today)

About the Author

ARMA International

Analytics 2021.02.01 What's Next in Information Governance? Continuous Audit and Analytics

Information Governance 2020.11.19 Information Governance: Alignment with Business is Essential

Information 2020.09.11 New Podcast Series Focuses on the Careers of Women Leaders in Information Governance

Taxonomy 2020.08.19 What Can We Learn About the IG Profession from the ARMA InfoCon 2020 Taxonomy