NATIONAL CAPITAL REGION
THREAT INTELLIGENCE CONSORTIUM

August 2, 2019

Intelligence Bulletin

Product No. 2019-08-031
NTIC SIN No. 2.7 | HSEC No. 7

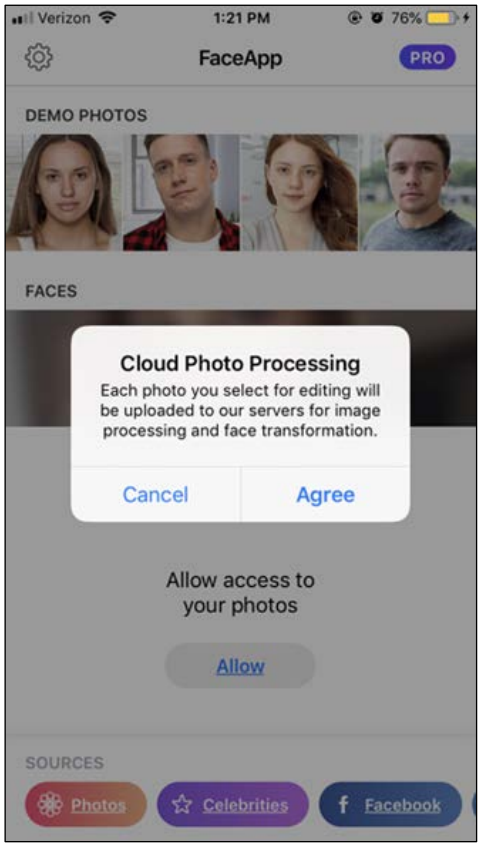
Securing Privacy Online: The "FaceApp Challenge"

A recent social media trend—the "FaceApp Challenge"—is raising questions about data privacy risks posed from sharing information with the Russia-based company, FaceApp, and underscores the need for the public to thoroughly read terms of service and privacy policies before using this, or any, application. FaceApp, which has attracted at least 80 million users worldwide, uses artificial intelligence on remote servers to alter an uploaded photo of a face so it appears to have aged. The outcry over FaceApp follows growing consumer concerns about the broad privacy and terms of use policies that allow Internet-based companies to use applications to track and/or sell user data to third parties. Companies purchase this type of data to gain insights into consumers' behavior and preferences, valuable for marketing and sales purposes.

- FaceApp's CEO claims the data is stored on US-based servers of companies such as Amazon. However, FaceApp's terms of use allow the company "perpetual" and "irrevocable" access to uploaded content and to transfer and store user data in the United States and other countries or anywhere there is a FaceApp facility. This provision could allow foreign governments, including Russia and its intelligence services, or other third parties to gain access to US citizens' user data.

- Company officials say FaceApp does not share data for ad-targeting purposes, but rather, the company earns its revenue through paid subscriptions for premium features. However, FaceApp's privacy policy specifically mentions the company may share certain information with third party ad networks, suggesting user data could be sold for advertising purposes.

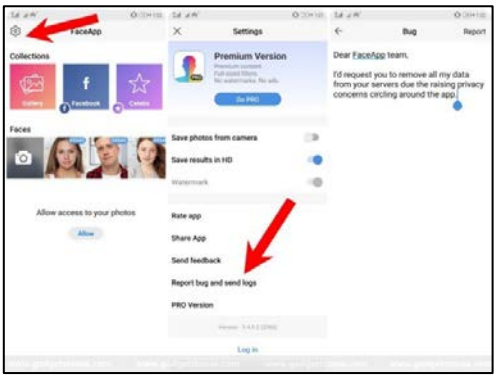
- When users upload facial images to FaceApp, they relinquish control of sensitive biometric data to a program that does not require explicit consent to reuse their image, potentially placing users at risk for identity theft.



Editing photos with FaceApp uploads user data to remote servers
(Source: Impact)

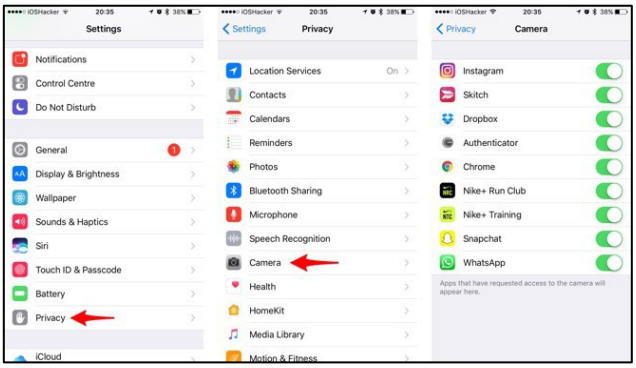
Protect Yourself When Using Applications

The NTIC recommends residents use the following guidelines to protect their data while using online applications.



(Source: Gadgets to Use)

Deleting the application does not prevent FaceApp from using data already uploaded. If you have already downloaded and used FaceApp, FaceApp accepts formal requests to delete data retroactively. ***Within the application: Settings> Report a bug and send logs > Use the word "privacy" in the subject line.*** Users may also email support@faceapp.com.



(Source: BytesIn)

Revoke an application's access to personal information or a feature such as your camera or location***. On an iPhone visit, Settings> Privacy> Camera (toggle on or off). On an Android visit, Settings> Apps> Configure Apps or App Settings> App Permissions.***

(Source: iGeeks)

Limit ad tracking. ***On an iPhone visit, Settings > Privacy > Advertising > Limit Ad Tracking. On an Android visit, Settings > Google > Ads > Turn on Opt Out of Ads Personalization.***

Additional Safety Practices

- ***Read*** the terms of service and privacy policy prior to using any application.
- ***Download*** a "Firewall" application such as Guardian Mobile Firewall to prevent data from leaving your phone.
- ***Delete*** any applications with concerning privacy policies.