Republika ng Pilipinas
KAGAWARAN NG KATARUNGAN
Department of Justice
Manila

DEPARTMENT OF JUSTICE
OFFICE OF CYBERCRIME
20 June 2020

PUBLIC ADVISORY ON FACEAPP – AI FACE EDITOR

This Public Advisory is issued by the Department of Justice (DOJ) – Office of Cybercrime (OOC) in response to the emerging cybersecurity risks associated with the FaceApp – AI Face Editor (FaceApp AI) application (app) developed by FaceApp Inc.

FaceApp AI is a photo filter app that allows users to improve the quality of their photos with impression filters, change in hair color and style, application of makeup, color filters, lens blur, and numerous other tools. FaceApp Inc. is a United States (US) entity that publishes and hosts the app. Its official business address is at 1000 N West Street, Suite 1200, Wilmington, Delaware, 19801, USA.

Based on an open source research, the DOJ-OOC found out that FaceApp Inc. complies with the EU-US and the Swiss-US Privacy Shield Frameworks as set forth by the US Department of Commerce. Said framework provides companies on both sides of the Atlantic with a mechanism to comply with data protection requirements regarding the collection, use, and retention of personal information from the European Union and Switzerland to the United States in support of transatlantic commerce.[1]

FaceApp AI's Privacy Policy was last updated on 04 June 2020[2]. Based thereon, when a user opted to subscribe to the said app, the following information may be collected for purposes of improving the app:

1. **Photographs you provide when you use the app**

   It is worth noting that only specific images the users choose to modify using the app are obtained by it. Thus, photo albums are not collected even if a user grants the app access thereto. Each photograph uploaded using the app is likewise encrypted, which key is stored locally on each user's device. This means that the only device that can view the photo is

[1] Retrieved on 20 June 2020 at https://www.privacyshield.gov/.
[2] Retrieved on 20 June 2020 at https://www.faceapp.com/privacy-en.html.

the device from which the photograph was uploaded using the app – the user's device.

Photographs are not used for any reason other than to provide the user with the portrait editing functionality of the app.

The app only uploads to the cloud the photographs that the users specifically select for editing. Uploaded photographs remain in the cloud for a limited period of 24-48 hours after the last edit to enhance user experience in case the user decided to return to the image and make additional changes.

2. **App usage information**

   The app collects information as to how the users use the app, including their preferred language and the date and time when they first installed and last used the app.

3. **Purchase history**

   This information is gathered as a confirmation that a user specifically subscribed to the paid version of the app – FaceApp Pro.

4. **Social media information**

   This block of information is only obtained by the app if a user choose to login via a third-party platform or social media network, such as Facebook.

   If a user chose to do so, the app will be able to collect information from the connected platform or network, such as social media alias, first and last name, number of "friends" on the social media platform and, depending on the user's Facebook or other network settings, a list of friends or connections.

5. **Device data**

   This information pertains to computer and mobile device operating system type and version number, manufacturer and model, device ID, push tokens, IP address and the associated country in which the user is located, and other information about the device you are using to visit the app.

6. **Online activity data**

   Such are information about the user's use of and actions on the app and the sites, including pages or screens viewed, how much time was spent on a page or screen, and navigation paths between pages or screens.

The foregoing information are likewise collected for purposes of compliance with government regulation, fraud prevention, and safety. Hence, personal information may be disclosed to law enforcement, government authorities, and private parties as necessary or appropriate to protect, investigate and deter against fraudulent, harmful, unauthorized, unethical or illegal activity.

ADVISORY

I. Make it a habit to read an app's Privacy Policy and Terms and Conditions before downloading it

This will give the user a sufficient amount of information on how an application operates and processes personal information submitted to it. At the very least, the processing of information must adhere to the principles of transparency, legitimate purpose and proportionality as provided for under Republic Act (R.A.) No. 10173 or the Data Privacy Act of 2012.

It turn, this information may be used as a baseline in deciding whether an app is safe and secure.

II. Avoid creating an account within an app by connecting it to third-party networks and platforms, such as Google and Facebook

When creating an account in any app, users must refrain from automatically connecting the new account to his/her existing accounts from third-party networks and platforms, such as Google and Facebook. This will keep the new app from harvesting vast information from a user's Google and Facebook accounts.

III. Always update the app you downloaded to its latest version

Every app connected to the internet is vulnerable to cyber attacks. It is crucial that users regularly update their apps once it is available. These software updates usually include patches to the app's reported vulnerabilities.

IV. Report any irregularities to the appropriate enforcement agencies

If a user encounters or obtains actual knowledge of any facts or circumstances that a certain app is being used by another user to harass, abuse, defraud, or commit harm against another, he/she is encouraged to report the said incident to the law enforcement agencies as soon as reasonably possible.

Users may report cybercrime and cyber-related incidents to the following enforcement agencies:

PHILIPPINE NATIONAL POLICE – ANTI-CYBERCRIME GROUP	Email Address:	acg@acg.pnp.gov.ph
	Mobile No.:	(+63) 998-598-8116
	Telephone Nos.:	(+632) 414-1560
	Website:	https://pnpacg.ph/main
	Facebook:	https://www.facebook.com/anticybercrimegroup/
NATIONAL BUREAU OF INVESTIGATION – CYBERCRIME DIVISION	Email Address:	ccd@nbi.gov.ph
	Telephone No.:	(+632) 8523-8231 to 38 local 3455
	Website:	www.nbi.gov.ph
DEPARTMENT OF JUSTICE – OFFICE OF CYBERCRIME	Email Address:	cybercrime@doj.gov.ph
	Telephone No.:	(+632) 8524-8216
	Website:	www.doj.gov.ph/office-of-cybercrime.html
	Facebook:	https://www.facebook.com/OfficeofCybercrimePH/

For your guidance and information.

ATTY. CHARITO A. ZAMORA
Officer-in-Charge
DOJ Office of Cybercrime