

# GUIDELINES ON MESSAGING APPS

Version 1.0

## **REVISION HISTORY LOG**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **LOG NO.** | **DATE** | **SECTION** | **DETAILS** | **AUTHOR** |
| 1 | 15 February 2021 | I-II and VII a. | Overview, Issue, Google Android Permissions | Kelvin Magtalas |
| 2 | 14 March 2021 | III-X | Definition of Terms, Scope, Objectives, Method, Added Apple iOS, Information Contained in App Stores, Analysis and Key Findings, Good Practice Guide for Developers and Users | Janssen Esguerra |
| 3 | 06 April 2021 | All | Revisions | Jonathan Ragsag |

**TABLE OF CONTENTS**

[GUIDELINES ON MESSAGING APPS 1](#_Toc66997916)

[REVISION HISTORY LOG 2](#_Toc66997917)

[I. OVERVIEW 4](#_Toc66997918)

[II. ISSUE 4](#_Toc66997919)

[III. DEFINITION OF TERMS 5](#_Toc66997920)

[IV. SCOPE 5](#_Toc66997921)

[V. OBJECTIVES 5](#_Toc66997922)

[VI. METHOD 5](#_Toc66997923)

[VII. INFORMATION CONTAINED IN APP STORES 6](#_Toc66997924)

[a. GOOGLE PLAY STORE (ANDROID OS) 6](#_Toc66997925)

[b. APPLE APP STORE (iOS OS) 7](#_Toc66997926)

[c. KEY FINDINGS 8](#_Toc66997927)

[VIII. PERMISSIONS SOUGHT BY MESSAGING APPS 8](#_Toc66997928)

[a. GOOGLE PLAY STORE 9](#_Toc66997929)

[b. APPLE APP STORE 9](#_Toc66997930)

[c. KEY FINDINGS 10](#_Toc66997931)

[IX. Good Practice Guides (GPG) 12](#_Toc66997932)

[a. For Messaging App Developers 12](#_Toc66997933)

[b. For Messaging App Users 13](#_Toc66997934)

[X. CONCLUSION 15](#_Toc66997935)

## **OVERVIEW**

**Messaging Apps**

Social messaging or chat applications, more commonly known as “messaging apps”, are software applications that provide instant messaging (IM) / real-time text transmission over the Internet.

The term instant messaging originated from the 1990s and predates the Internet. Early programs were primarily real-time, as characters appeared as they were typed.

In the emergence of smart phones in the late 2000s and early 2010s, numerous startups developed online mobile messaging apps that replaced instant messaging and SMS.

*Emergence of online messaging apps in early 2010s*

In the first week of January 2021, WhatsApp briefly became a trending app among its users because of its new privacy policy.

WhatsApp Inc. gave the users at least three months to properly review and accept the policy following user backlash and confusion. WhatsApp was forced to explain what data it collects and how it shares that information with its parent company, Facebook Inc.

## **ISSUE**

WhatsApp announced that its privacy policy update will take effect on 15 May 2021 instead of 08 February 2021 which was the previously set date.

The updated policy terms informed users that WhatsApp receives information from, and shares information with, the Facebook family of companies. These changes were focused on introducing new options for businesses using WhatsApp Business.

WhatsApp claims that its messaging platform is end-to-end encrypted, meaning only the sender and recipient can read the message and it is not stored on Facebook servers. But WhatsApp is also pushing messaging for businesses aggressively. The updated privacy policy was intended to alert users that some businesses would soon be using Facebook-owned servers to store messages with customers. Facebook has already said that it will not access those messages for any type of ad targeting or profiling, but the language in the updated terms of service concerned many users who worry that Facebook would suddenly view or access their private messages.

## **DEFINITION OF TERMS**

1. **App store (or app marketplace)** is a general term for a type of digital distribution platform or a digital shop where users can buy & download digital software and applications.
2. **App** **(abbreviation for application)** refers to a software that provides additional functionality to an operating system. The term app originally referred to any mobile or desktop application. But as more app stores have emerged to sell mobile apps to smartphone and tablet users, the term has evolved to refer to a small program that can be downloaded and installed all at once.
3. **OS (abbreviation for Operating System)** refers to the software that allows a user to run other apps on a computing device such as a smartphone.
4. **Smartphone** is a mobile phone with highly advanced features. A typical smartphone has a high-resolution touch screen display, Wi-Fi connectivity, web browsing capability, and the ability to accept sophisticated apps. The majority of these devices run on any of these popular mobile OS: Android, Symbian, iOS, BlackBerry OS and Windows Mobile.

## **SCOPE**

These guidelines apply only to the mobile versions of the messaging applications. Desktop versions of the messaging applications are excluded from these guidelines.

## **OBJECTIVES**

In view of the foregoing, these guidelines aim to provide readers with information and awareness on the following:

1. general information given by app stores;
2. permissions sought by each messaging app;
3. categories of personal information of data subjects that the messaging apps process; and
4. good privacy practices in the use of messaging apps.

## **METHOD**

To be able to provide key findings and recommendations, six (6) messaging apps on Google’s Android OS and Apple’s iOS OS were sampled. The rationale for their sampling or selection is due to their popularity and use in the Philippines. The following messaging apps on [Google Play Store](https://play.google.com/store) (for the Android OS) and [Apple App Store](https://www.apple.com/ph/app-store/) (for the iOS OS) were assessed:

|  |  |
| --- | --- |
| 1. Messenger; | 4.) WhatsApp; |
| 1. Telegram; | 5.) WeChat; and |
| 1. Viber; | 6.) Signal |

## **INFORMATION AVAILABLE ON THE APP STORES**

Each app store uniquely presents the mobile apps that are available. Tables 1 and 2 below enumerate and describe the information available on Google Play Store and Apple App Store, respectively:

### **GOOGLE PLAY STORE (ANDROID OS)**

|  |  |
| --- | --- |
| **Top Information** | **Brief Description** |
| Icon | Icon image of the app |
| Name | Name of the app |
| Offered by | Entity name of the app developer/provider |
| Category | Category of the app where it is classified or tagged under |
| Age Rating | Provides age-based rating |
| Average Users’ Rating | Average score given by the users who chose to rate the app in 1-5 stars, where 5 is the highest rating |
| Screenshots | Screen captures of the app with featured introductory functions |
| Introduction | Provides an overview of the app |
| Reviews | Provides user ratings and reviews on the app |
| **Additional Information** | |
| Updated | Date when the app is updated to its latest version |
| Current Version | Refers to the latest build or version number of the app |
| Interactive Elements | Include things like whether an app shares a user's location, or if it allows users to interact with each other, i.e.: users interact, shares location, in-app purchases, etc. |
| Report | Provides avenues for [reporting content issues or violations](https://support.google.com/googleplay/answer/2853570?visit_id=637513317540950601-2047828573&p=report_content&rd=1&co=GENIE.Platform%3DAndroid&oco=1) |
| Size | Approximate size of the applications in megabytes (M) or gigabytes (G) |
| Requires Android | Minimum build or version number of the Android OS to run this app |
| In-app Products | Approximate cost range of in-app purchases available on the app |
| Offered By | Name of the application developer |
| Installs | Approximate number of user installs |
| Content Rating | Provides [content rating of the app](https://support.google.com/googleplay/answer/6209544?p=appgame_ratings&visit_id=637513317540950601-2047828573&rd=1), which varies by age of users, its interactive features, and rating regulations by country or region |
| Permissions | Lists all of the permissions required in using the app |
| Developer/s | Provides links to the providers’/developers’ website, email address, privacy policy and location |

*Table 1. Google Play Store information on an app*

### **APPLE APP STORE (iOS OS)**

|  |  |
| --- | --- |
| **Top Information** | **Brief Description** |
| Icon | Icon image of the app |
| Name | Name of the app |
| Offered by | Entity name of the app developer |
| Category | Category of the app where it is classified or tagged under |
| Age Rating | Provides age-based rating |
| Average Users’ Rating | Average score given by the users who chose to rate the app, in 1-5 stars, where 5 is the highest rating |
| Screenshots | Screen captures of the app with featured introductory functions which vary among Apple devices: iPhone, iPad and Apple Watch |
| Introduction | Provides an overview of the app |
| What’s New | Provides description and extent of the changes that the developer made on the current version of the app |
| Version | Refers to the latest build or version number of the app |
| Version History | Provides a list of all the app versions that were released |
| Ratings and Reviews | Provides user ratings and reviews on the app |
| App Privacy | Provides a link to the developer’s privacy policy, [Privacy Definitions and Examples](https://apps.apple.com/story/id1539235847), [‎Learn More About App Privacy : App Store Story (apple.com)](https://apps.apple.com/story/id1538632801), Data Used to Track You, Data Linked to You, and Data Not Linked to You |
| **Additional Information** | |
| Provider | Entity name of the app developer/provider |
| Compatibility | Minimum build or version number of the iOS OS to run this app |
| Location | Provides notice on how the app uses the device’s location |
| Size | Approximate size of the applications in megabytes (MB) or gigabytes (GB) |
| Languages | Available languages that the app can be used to display |
| Copyright | Provides copyright information |
| Category | Category of the app where it is classified or tagged under |
| Age Rating | Provides age-based rating and description |
| Price | Specifies whether the app is free to use and install or requires payment before use and install |

*Table 2. App Store information of an app*

### **KEY FINDINGS**

1. One of the general data privacy principles of the Philippines’ Data Privacy Act of 2012 (DPA) and most data protection regimes around the world is transparency. Therefore, the messaging apps provide a common and standard set of information that data subjects or users ought to know before deciding to give their consent: to install the app, allow permissions sought by the app, provide personal information and use the app occasionally or regularly.

“Top Information” refers to the most important information at the top portion of the landing page of the app while “Additional Information” refers to other useful information regarding the app.

For users, the most important details available on the app stores are as follows:

1. permissions sought (whether these are excessive based on the app’s purpose/s or functionalities);
2. other user ratings and reviews (for user experience red flags);
3. content/age rating (whether the app is suitable for minors or children); and
4. the privacy policy (which contains the overall information on privacy and data protection).
5. Some details under top information are also posted under additional information, showing the importance of these to app users. They are as follows:
   1. Developer (Google Play Store) and Provider (Apple App Store) – usually denotes the Personal Information Controller;
   2. App Category – reveals the purpose of the app;
   3. Content/Age Rating – minimum maturity level of content provided by the apps; and
   4. Whether the app is free or offers in-app purchases.

## **PERMISSIONS SOUGHT BY MESSAGING APPS**

Each app store uniquely discloses the permissions requested by messaging apps or apps in general. Tables 3 and 4 show the permissions sought by the Android OS version of the app and the iOS version of the app, respectively.

### **GOOGLE PLAY STORE**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Messaging Apps** | Facebook Messenger | Telegram | Viber | WhatsApp | WeChat | Signal |
| **Permissions** | | | | | | |
| WiFi |  |  |  |  |  |  |
| Contacts |  |  |  |  |  |  |
| SMS |  |  |  |  |  |  |
| Phone |  |  |  |  |  |  |
| Microphone |  |  |  |  |  |  |
| Device ID & call information |  |  |  |  |  |  |
| Location |  |  |  |  |  |  |
| Calendar |  |  |  |  |  |  |
| Camera |  |  |  |  |  |  |
| Device & app history |  |  |  |  |  |  |
| Photos/Media/Files |  |  |  |  |  |  |
| Identity |  |  |  |  |  |  |
| Wearable sensors/Activity data |  |  |  |  |  |  |
| Other |  |  |  |  |  |  |

*Table 3. Permissions sought by messaging apps on Google Play Store*

### **APPLE APP STORE**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Messaging Apps** | Facebook Messenger | Telegram | Viber | | | WhatsApp | WeChat | | Signal |
| **Data Used to Track You** |  |  |  | | |  |  | |  |
| **Data Linked to You** |  |  |  | | |  |  | |  |
| **Data Not Linked to You** |  |  |  | | |  |  | |  |
| **Permissions** | | | | | | | | | |
| Browsing History |  |  |  |  |  |  |  |  |  |
| Contact Info |  |  |  |  |  |  |  |  |  |
| Contacts |  |  |  |  |  |  |  |  |  |
| Diagnostics |  |  |  |  |  |  |  |  |  |
| Financial Info |  |  |  |  |  |  |  |  |  |
| Health & Fitness |  |  |  |  |  |  |  |  |  |
| Identifiers |  |  |  |  |  |  |  |  |  |
| Location |  |  |  |  |  |  |  |  |  |
| Other Data |  |  |  |  |  |  |  |  |  |
| Purchases |  |  |  |  |  |  |  |  |  |
| Search History |  |  |  |  |  |  |  |  |  |
| Sensitive Info |  |  |  |  |  |  |  |  |  |
| Usage Data |  |  |  |  |  |  |  |  |  |
| User Content |  |  |  |  |  |  |  |  |  |

*Table 4. Permissions sought by messaging apps on Apple App Store*

### **KEY FINDINGS**

1. The Apple App Store app permissions can be found on App Privacy>See Details. The App Privacy of the Apple App Store has three (3) categories of permissions sought, branded as “Privacy Nutrition Labels[[1]](#footnote-2)”:
   * 1. Data Used to Track You – data may be used to track you across apps and websites owned by other companies;
     2. Data Linked to You – data may be collected and linked to your identity; and
     3. Data Not Linked to You – data may be collected but not linked to your identity.

The Google Play Store app permissions can be found on ADDITIONAL INFORMATION > View details.

Both app stores have indicated specific permissions sought by messaging apps and their descriptions. However, in terms of demonstrating transparency and adequately informing the data subjects, Apple/App Store/iOS has the edge. By being granular while maintaining a clear and plain language, it is a trailblazer in this aspect. While Google/Play Store/Android OS lags currently, it is now working on its own “privacy nutrition labels[[2]](#footnote-3)”.

1. The Google App Store and the Apple App Store both provide a breakdown of permissions sought by each messaging app. While both have a common and standard set of terminologies used, they differ in nomenclature. Some names of permissions may be synonymous with each other in both app stores, i.e.: the permission “Photos/Media/Files” on the Google Play Store is equivalent to “User Content” on the Apple App Store and “Device ID & call information” on the Google Play Store is equivalent to “Identifiers” on the Apple App Store.
2. Common Permissions sought by messaging apps (6/6): WiFi, Contacts/Contact Information, Phone, Microphone, Device Identifiers & Call Information, Camera, Photos/Media/Files, Identity and Other are expected permissions due to the minimum functionality or actions users perform when interacting or using a messaging app, i.e.: WiFi is needed to establish connection to the internet, Phone/Microphone are needed to transmit and receive voice or audio data, Camera/Files are needed to transmit or receive photo or video data, etc.
3. Identity (6/6): All messaging applications use this permission. It provides phone status and identity. This works by processing the unique identifier associated to a user’s mobile device, the International Mobile Equipment Identifier (IMEI).
4. Location Permission (5/6): Signal is the only messaging app that does not collect location information. Most of the apps listed here collect location information primarily because of the application function that sends the exact location, for example in meetups.
5. Device & App History Permission (4/6): Allows the app to retrieve information about currently and recently running tasks. This may allow the app to discover which applications are used on the device. This is a spyware-like permission that has been deprecated by Android[[3]](#footnote-4). Possible reasons why developers have not totally removed this permission are debugging, testing, or backward compatibility on legacy Android OS versions.
6. SMS Permission (3/6): Granting SMS permission will enable the applications to read the inbox and send & receive SMS messages. Messenger, WhatsApp, and Signal may require access to the device’s SMS inbox if a user chooses to use either one of them as the default SMS client/app.
7. Wearable Sensors / Activity Data (1/6): Among the messaging apps, only WeChat has access to this permission. This may be attributed to the “WeRun” fitness module or plugin integrated in WeChat. It is mainly touted for fitness tracking and health.
8. Other: Both iOS OS and Android OS messaging apps have permission for “Other”. All uncategorized permissions are lumped and itemized under this permission.

## **Good Practice Guides (GPG)**

### **For Messaging App Developers**

Build privacy in the core of app development (privacy by design). Privacy should not just be an afterthought.

1. **Request minimum permissions**. Every time you’re asking for a permission, you are forcing users to decide. Reduce the user’s burden. If your app really needs to access a specific permission, ask it in increments. Look for alternatives in use cases that will help limit the number of permissions you ask. Use statistics to derive the rate of denial of a specific permission and influence subsequent updates & approach to that permission.
2. **Ask for access only in context**. Ask for a specific permission, when the in-app features demand for it, only due to a user action (i.e., in meetups, users press location sharing in their messaging apps to know their proximity or location relative to each other). Tweak the user interface in such a way that it provides appropriate explanation to the user and is designed to never be forced or accidentally permitted.
3. **Plan for users to select deny**. Whenever possible, minimize the time or access window of application permissions. Let the user choose to allow a permission through any of the following options:
   * + **While using the app**. Once the user selects this option, the messaging app will have access to the specific permission only if the app is in the foreground or active window or in use.
     + **Only this time**. The messaging app will have access only for a short period and access will automatically be revoked.
     + **Deny**. Access of the messaging app to the requested permission is denied.
       - Handling “deny”
         * **Do not block users from using your app**. There are instances when the app forces users to allow the requested permission or else the users won’t be able to use the app at all. Users must still be able to use the app (ex. denying microphone or storage permission will still let users browse their messages and chat through the messaging app).
         * **Expect permanent deny**, don’t push users to settings. Ask for permission in context and allow the permission to be declined within the app interface.
4. **Access sensitive permissions only when the user expects it**. The messaging app must be able to provide instantaneous apermissccess to sensitive permissions such as camera and microphones. It must provide continuous visual indicators that applications are actively accessing these permissions.
5. **Pay attention to libraries**. Audit current data especially sensitive data accessed by third-party API and libraries.

### **For Messaging App Users**

Take note that these are guidelines and your specific needs may vary depending on your risk appetite.

#### **Messenger (Facebook)**

* Preferably, access your Facebook messages using a browser or the “lite” version of Facebook Messenger.
* Preferably, use “Messenger Kids” for children.
* Profile: Set Active Status: Off
* Privacy:
  + Message Delivery
    - Friends of Friends on Facebook: Don’t Receive Requests
    - Your followers on Instagram: Don’t Receive Requests
    - Others on Facebook and Instagram: Don’t Receive Requests
  + Story Audience: Friends Only
  + SMS: Off
* Contacts: Set Sync Contacts to off
* Photos and Media: Open Links in Default Browser: On

#### **Telegram**

* + Privacy
    1. Phone Number: Nobody
    2. Last Seen & Online: Nobody
    3. Profile Photos: My Contacts
    4. Forwarded Messages: Nobody
    5. Calls: Nobody
    6. Groups
       1. Who can add me to group chats: My Contacts
  + Security
    1. Passcode Lock: On
       1. Unlock with fingerprint: Off
       2. Show app content in Task Switcher: Off
    2. Two-Step Verification: On
    3. Review all active sessions and terminate those that are unknown or inactive to you
    4. Set a preferred period for Account Self-Destruct
    5. Contacts
       1. Sync Contacts: Off
       2. Suggest Frequent Contacts: Off

#### **Viber**

* + Viber backup: Chat back up is discouraged since it will link to your Google Drive.
  + Desktop and tablets: Review active logins and deactivate sessions that are unknown or inactive to you.
  + Privacy
    1. Share online status: Off
    2. Send “seen” status: Off
    3. Show your photo: Off
    4. Share your birth date: Off
    5. Auto spam check: On
    6. Use peer-to-peer: Off
    7. Allow friend suggestions: Off
    8. Trusted Contacts: Off
    9. Control who can add you to groups: My contacts
    10. Personal data
        1. Collect analytics: Off
        2. Allow content personalization: Off
        3. Allow accurate location-based services: Off

#### **WhatsApp**

* + Privacy
    1. Last seen: Nobody
    2. Profile photo: Nobody
    3. About: Nobody
    4. Read receipts: Off
    5. Groups: My contacts
    6. Live location: None
    7. Fingerprint lock: Disable
  + Security
    1. Show security notifications: On
    2. Two-step verification: On
  + Request account info: Request report to see what data WhatsApp holds about you.
  + Chat back up is discouraged since it will link to your Google Drive.

#### **WeChat**

* + Privacy
    1. Friend Confirmation: On
    2. Methods for friending me
       1. WeChat ID: Off
       2. Mobile: Off
       3. Group Chat: Off
       4. QR Code: Off
       5. Contact Card: Off
    3. Moments and Time Capsule
       1. Hide My Posts: Choose contacts who could not watch your Moments posts.
       2. Hide Their Moment: Choose contacts whose Moments you do not want to see.
       3. Viewable by Others: Limit the period of Moments that are viewable to others.

#### **Signal**

* + Privacy
    1. App access
       1. Screen lock: On
       2. Screen lock inactivity timeout: Put a screen lock period
       3. Screen security: On
       4. Incognito keyboard: On
    2. Communication
       1. Always relay calls: On
       2. Read receipts: Off
       3. Typing Indicators: Off
       4. Generate link previews: Off
    3. Signal PIN
       1. PIN reminders: On
       2. Registration Lock: On

## **CONCLUSION**

* Less is more when it comes to privacy of messaging apps. Parents should review the settings of their children’s’ messaging apps and tweak them according to this guide.
* Review the permissions of messaging apps. Grant the minimum permissions needed to be able to use the append and revoke permissions that are not in use. Allow them only in the instance that you are going to use them although this may be a tedious task and places a burden on the user. Developers of operating systems of smart phones are enjoined to provide options to users in granting instantaneous access to the permissions and automatically revoking them after use.
* Be vigilant when conversing with strangers. Verify their identities first before providing any information about yourself.
* Do not tap links & files in messaging apps if you are not expecting them and especially if they came from a stranger. You can be phished, or a malware can infect your device.
* Be careful in joining a group as all group members will gain access to your phone number.

1. [Apple's Privacy Nutrition Labels, available now and good for business | Computerworld](https://www.computerworld.com/article/3600998/apples-privacy-nutrition-labels-available-now-and-good-for-business.html) [↑](#footnote-ref-2)
2. [Google is working on its own privacy 'nutrition' labels for the Play Store | Android Central](https://www.androidcentral.com/google-working-its-own-privacy-nutrition-labels-play-store) [↑](#footnote-ref-3)
3. <https://developer.android.com/reference/android/app/ActivityManager.html#getRunningTasks(int)> [↑](#footnote-ref-4)