ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 移动智能终端的移动互联网应用程序（App）个人信息处理活动管理指南

Information security technology—Personal information processing management guide for Apps of smart mobile terminals

（征求意见稿）

（本稿完成时间：2022 年 5 月 26 日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：华为技术有限公司、中国电子技术标准化研究院、中国网络安全审查技术与认证中心、OPPO 广东移动通信有限公司、维沃移动通信有限公司、北京小米移动软件有限公司、荣耀终端有限公司、北京三星通信技术研究有限公司

本文件主要起草人：衣强、何延哲、胡影、刘行、周晨炜、樊华、李腾、张玮、任冠一、赵晓娜、吴越。

引　言

随着移动互联网的迅速发展，移动互联网应用程序给人们生活带来便利的同时，越来越多地处理人们的个人信息，但也存在个人信息不合理收集、使用的问题，移动终端作为移动互联网应用程序的载体，通过移动终端及其上操作系统的相应机制可在一定程度上管理个人信息的收集使用，帮助移动互联网应用程序合理的收集使用个人信息。

为保障移动智能终端用户的合法权益，促进个人信息的合理利用，根据《中华人民共和国个人信息保护法》，本文件按照移动互联网应用程序在移动智能终端上的生命周期节点，提出移动智能终端的个人信息安全管理措施，增强 App 处理个人信息行为明示程度，为 App 用户提供更多个人信息保护控制机制，以加强移动终端操作系统上运行的移动互联网应用程序的个人信息安全。

信息安全技术 移动智能终端的移动互联网应用程序（App）个人信息处理活动管理指南

1 范围

本文件针对移动智能终端提供了App个人信息安全功能设计、管理个人信息安全风险的指南，以增强App收集个人信息行为的明示程度，并为App用户提供更多个人信息保护方面的控制机制。

本文件适用于指导移动智能终端提供者进行系统设计、开发活动，主要适用于智能手机。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

移动智能终端 mobile smart terminal

接入公众移动通信网络、具有操作系统、可由用户自行安装和卸载应用软件的移动通信终端产品。

[来源：GB/T 34976—2017，3.1]

3.2

移动智能终端操作系统 smart mobile terminal operation system

移动智能终端最基本的系统软件，控制和管理终端上的各种硬件和软件资源，并提供应用程序开发的接口。

注 1：一般包括移动智能终端图形交互系统 GUI、核心功能库、应用框架、安全套件、业务模型组件、核心业务功能、基础应用软件等多层架构和软件实体。

注 2：基础应用软件一般包括移动智能终端操作系统基本功能及服务，如实现移动通信基本功能、系统管理功能、多媒体服务功能、用户交互入口、保障数据安全功能、安全管理功能等。

[来源：GB/T 34976—2017，3.2，有修改]

3.3

移动互联网应用程序 mobile internet application；App

运行在移动智能终端上的应用程序。

注：包括移动智能终端预置、下载安装的应用程序和小程序。

[来源：GB/T 34976—2017，3.2，有修改]

3.4

预置应用软件 pre-installed application

由移动智能终端生产企业预置，在移动智能终端主屏幕或辅助屏幕界面内存在用户交互入口，为满足用户不同的应用需求而提供的、可独立使用的软件程序。

3.5

小程序 mini program

基于应用程序开放接口实现的，用户无需安装即可使用的移动互联网应用程序。

注：应用程序通过公开其应用程序编程接口（API）或函数，使外部的程序可以增加该应用程序的功能或使用该应用程序的资源，而不需要更改该应用程序的源代码。

3.6

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

[来源：GB/T 35273—2020，3.1，有修改]

3.7

敏感个人信息 sensitive personal information

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

注：个人敏感信息包括身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14 岁以下（含）儿童的个人信息等。

[来源：GB/T 35273—2020，3.2，有修改]

3.8

个人信息处理活动 personal information processing

个人信息的收集、存储、使用、加工、传输、提供、公开、删除等活动的总称。

注：也称“个人信息处理行为”。

3.9

敏感系统权限 sensitive system permission

移动智能终端向移动互联网应用程序开放的，调用个人信息或系统敏感资源的能力。

注：包括但不限于涉及通讯录、本机号码、短信、日历、打电话、发短信、存储等相关的权限，也称“可收集个人信息权限”。敏感系统权限示例见附录 A。

3.10

应用程序列表 application list

移动智能终端上已安装应用程序的描述信息集合。

注：例如已安装应用程序的名称、包名、版本等。

3.11

热更新 hot update

应用软件通过动态发代码的方式，在不发布新版本的情况下进行应用更新，该过程无需重启应用软件或资源包。

4 缩略语

下列缩略语适用于本文件。

IMEI：国际移动设备识别码（International Mobile Equipment Identity）

MAC：媒体访问控制（Media Access Control）

5 总则

移动智能终端对App个人信息处理活动的管理宜遵循以下原则：

a) 公开透明：以合理方式记录、提示 App 处理个人信息情况，确保用户对 App 个人信息处理行为可感知；

b) 方便管理：向用户提供 App 个人信息管理入口，确保用户能方便地允许或拒绝 App 对个人信息的处理；

c) 确保安全：确保用户安装安全的 App，以及 App 以安全的方式处理个人信息；

d) 细致管控：对于移动智能终端上敏感度较高的个人信息，实施限制处理、细粒度管理等措施；

e) 合理适度：采取合理的手段管理其上个人信息，实现用户对个人信息管控的同时，避免对用户造成干扰（如频率过高的弹框提示等），影响 App 的正常运行。

6 移动智能终端上的 App 个人信息处理活动安全风险

按照App在移动智能终端上的运行程序，其生命周期可分为安装、启动、运行、更新、退出、停用/卸载阶段（见图1），各阶段主要面临的个人信息安全风险如下：

a) 安装阶段：用户安装来自未知渠道的 App 中包含病毒木马漏洞，导致终端上的用户个人信息被 App 窃取、滥用，以及 App 在安装时以捆绑形式要求用户一次性授予权限申请，导致不合理使用用户个人信息等；

b) 启动阶段：App 在用户不知情的情况下自启动或被关联启动，并且在启动后未经用户同意处理用户个人信息；

c) 运行阶段：App 未经用户同意或超出服务功能所必须范围处理个人信息，或强迫用户同意提供个人信息等；

d) 更新阶段：App 通过更新或热更新引入病毒、漏洞等，导致用户个人信息被窃取、滥用；

e) 退出/卸载阶段：App 退出/停用后未及时删除临时存储的个人信息，以及 App 卸载后未删除所存储的个人信息，存在可能被其它 App 利用的风险。

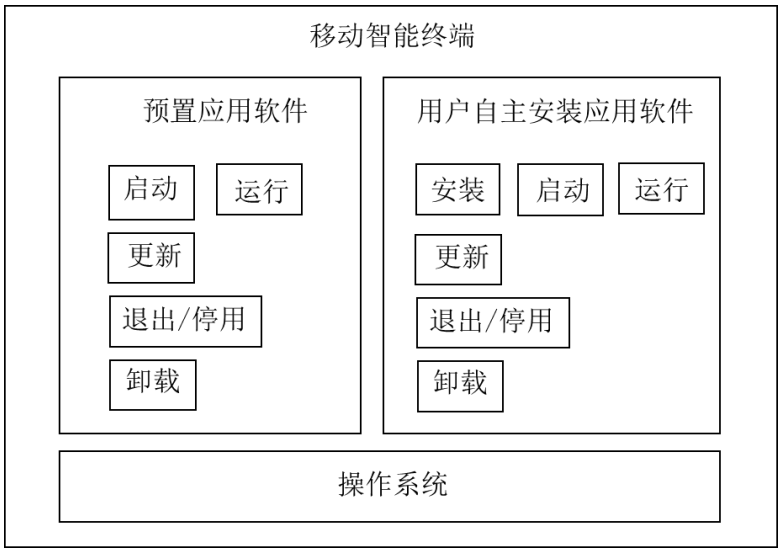

图1 App在移动智能终端上的生命周期

7 移动智能终端管理措施

7.1 透明化展示个人信息处理活动

7.1.1 App 使用个人信息提示

App持续或频繁调用敏感系统权限期间（如调用麦克风、相机、位置权限），移动智能终端宜提供展示指示标识的功能，需要考虑的要素如下：

a) 指示标识展示方式。在屏幕显著位置展示，包括但不限于在屏幕上方状态栏、角落采用彩色图示或下拉栏等；
b) 指示标识展示时机。App 前台和后台运行时，均向用户提示 App 正在使用敏感系统权限。
c) 权限查询及调整。可向用户提供查询正在使用敏感系统权限的 App 名称，并可对权限授权状态进行调整；
d) 指示标识含义简介。可向用户提供指示标识含义简介信息。

注：频繁调用指调用间隔小，向用户呈现持续调用的效果。

7.1.2 App 调用个人信息行为记录

移动智能终端对App行为进行记录，并设置统计、查询界面，为用户直观呈现个人信息调用情况，需要考虑的要素包括以下内容。

a) 记录的对象，包括：
   1) 移动智能终端上运行的第三方应用软件；
   2) 可选包括涉及个人信息处理活动的预置应用软件。
b) 统计和记录的行为，包括：
   1) 读取位置数据，读写通讯录数据、读取媒体影音数据（如照片、音频和视频）、读取短信，读取生物特征数据，读取唯一设备识别码（如 IMEI、WLAN MAC 地址），调用录音、拍摄、后台截屏/录屏行为；
   2) 可选记录读取应用程序列表、读取剪切板等；
   3) App 自启动、被关联启动的行为，为用户呈现自启动、被关联启动情况。

c) 记录展示的信息，包括：
   1) 调用行为按总量统计时，展示信息包括 App 名称、App 版本、调用行为名称、总量数据；
   2) 调用行为按次数统计时，展示信息为最后一次详情或每次详情，展示信息包括 App 名称、App 版本、调用行为名称、调用行为起始时间（展示时间精度至少为分钟）；
   3) App 存在频繁读取位置、媒体影音数据的情况，为避免向用户展示大量无效信息，可展示最后一次详情或一定周期内的总量，其它行为宜展示每次详情。
   4) 移动智能终端保存 App 调用个人信息行为的周期不少于 7 天，同时根据终端配置水平的差异，设定调用行为保存次数阈值。

注：保存次数阈值和保存周期取其中的最小值作为移动终端保存 App 调用行为记录的存储期限。

7.1.3 用户个人信息集中展示

移动智能终端宜在操作系统设置界面的二级目录中显著位置展现系统中的各类个人信息保护功能，具体包括：

a) 查看 App 收集个人信息行为记录情况；
b) 权限等与个人信息相关操作的管理界面。

7.2 App 个人信息处理行为管理

7.2.1 唯一设备识别码访问控制

移动智能终端宜针对不可变更、可变更唯一设备识别码建立访问控制机制，具体包括：

a) 限制 App 获取不可变更唯一设备识别码，如 WLAN MAC 地址、IMEI 等；
b) 广播 WLAN MAC 地址时，提供唯一设备识别码随机化的机制；
c) 为用户提供可便捷地重置可变唯一设备识别码（如广告标识符）的机制；
d) 可选支持用户选择是否允许将不可变更唯一设备识别码向 App 开放。

7.2.2 敏感数据访问提示和控制

移动智能终端宜向用户提供对移动智能终端上敏感数据/能力的访问提示和访问控制机制（敏感数据/能力示例见附录B），具体包括以下机制：

a) 对 App 获取应用程序列表的授权机制。授权方式包括始终允许、拒绝，可包括仅在使用中允许；

注：移动智能终端操作系统调用应用软件列表为用户呈现已安装应用，及实现应用安装、升级、使用等管理、备份、应用安全管理等功能的场景可作为例外。

b) 剪切板访问提示机制。当 App 读取剪切板时向用户提示；
c) 屏幕截图访问提示机制。当 App 调用屏幕截图功能获取屏幕截图时向用户提示；
d) 图片附加信息访问控制机制。当用户 App 通过系统相册/图库功能分享图片时，为用户提供去除照片附加信息的选项。附加信息包括拍摄参数、位置等；
e) 位置信息细粒度访问控制机制。当 App 访问用户位置信息时，为用户提供选择授予粗略位置或精准位置，以及是否允许后台访问位置的选项；
f) 用户相册细粒度访问控制机制。当用户主动选择特定图片、视频，并使用上传、分享特定图片、视频（非全量图片、视频数据）等功能时，支持在无需用户授权“相册/照片”、“多媒体”或“存储”等权限的情况下，允许 App 访问用户选择的特定照片、视频数据；
g) 通讯录细粒度访问控制机制。当用户主动选择特定联系人，并使用上传、分享特定联系人信息（非全量联系人）等功能时，支持用户在无需授权“通讯录”权限的情况下，允许 App 访问特定联系人数据；

h) 短信和通话记录访问控制限制。限制 App 向用户申请短信、通话记录权限，其基本功能为短信、电话应用除外；
i) 无需权限的拨打电话与发送短信机制。提供拨打电话与发送短信的公共接口，App 调用后跳转到系统提供的拨打电话、发送短信人机交互界面，实现用户主动操作完成拨打电话、发送短信功能；
j) 限制 App 在后台启动麦克风的能力；
k) 限制 App 在后台启动相机的能力；
l) 限制 App 在后台访问剪切板的能力；
m) 限制 App 首次在后台申请获得应用程序列表信息的能力。

7.2.3 存储空间使用

移动智能终端宜限制App对公共存储区及其他App私有存储目录下文件的访问，使得：
a) App 对存储空间的访问范围仅限于私有存储目录的文件以及用户授权后的公共存储区中的媒体文件（照片、视频、音频等）；
b) App 私有存储目录不能被其它 App 访问。

7.2.4 App 安装风险管理

用户通过网站、应用商店等移动应用分发平台下载、安装App时，移动智能终端宜：
a) 在执行 App 安装前明确提示用户并取得用户授权；
b) 判断所安装的 App 是否存在病毒、漏洞等安全风险，对于明确存在安全风险的 App 提示用户相应的安全风险，并提供阻止继续安装的选项；
c) 判断 App 是否存在可能的安全风险，若存在可能的安全风险提示用户，并提供其它渠道下载、安装、升级选项；
d) 判断 App 所声明权限是否包括敏感系统权限，不在安装阶段要求用户对敏感系统权限进行授权。

7.2.5 App 更新风险管理

移动智能终端宜通过技术、管理手段限制App热更新，避免通过热更新对用户个人信息权益造成损害。

7.2.6 App 退出/停用及卸载风险管理

移动智能终端宜提供以下机制：
a) 用户退出/停用 App 后，限制 App 的个人信息收集行为；
b) App 卸载时，提供彻底删除 App 私有存储目录下数据的机制。

7.3 用户控制 App 收集个人信息行为

7.3.1 系统权限能力增强

移动智能终端宜在权限申请授权粒度、权限使用等方面提供相应增强机制，包括：
a) 单次使用的授权方式。例如在 App 申请位置、相机、麦克风时，为用户提供本次使用授权的选项，当用户再次启动 App 时，需要重新询问用户是否允许其获取权限；
b) 仅在使用期间允许的授权方式，指仅当 App 处于前台运行状态时允许访问；

c) 权限申请目的可编辑，指支持 App 编辑权限申请目的说明，在 App 申请权限时的弹窗中予以展示；

d) 权限自动重置机制，指当用户长期（如 3 个月）未使用某 App，为用户提供自动将该 App 已开启的敏感系统权限重置为禁止状态。

注：用户可以通过交互式界面选择手动开启或关闭该功能。

7.3.2 App 自启动与关联启动管理

移动智能终宜为用户提供管理 App 自启动、被关联启动等行为的控制选项，选项的默认设置为关闭状态，或在 App 首次自启动、被关联启动时提示用户，由用户选择是否允许自启动、被关联启动。

7.4 预置应用软件处理个人信息行为管理

移动智能终端预装应用软件处理个人信息应具备合法性基础，以同意为合法性基础的情况，需获得用户同意后才能处理个人信息，不允许未经用户同意处理个人信息、不提供撤回同意选项。

附 录 A
（资料性）
操作系统权限名称命名及功能描述参考示例

安卓系统权限名称命名及功能描述参考示例见表 A.1。

表 A.1 安卓系统权限名称命名及功能描述参考示例

序号	权限分组	权限名	权限功能描述
1	CALENDAR 日历	READ_CALENDAR 读取日历	允许 App 读取用户日历数据
2		WRITE_CALENDAR 编辑日历	允许 App 写入用户日历数据
3	CALL_LOG 通话记录	READ_CALL_LOG 读取通话记录	允许 App 读取用户通话记录
4		WRITE_CALL_LOG 编辑通话记录	允许 App 写入用户通话记录
5		PROCESS_OUTGOING_CALLS 呼叫控制	允许 App 查看正在拨打的号码，并控制或终止呼出电话
6	CAMERA 相机	CAMERA 拍摄	允许 App 使用摄像头
7	CONTACTS 通讯录	READ_CONTACTS 读取通讯录	允许 App 读取用户通讯录
8		WRITE_CONTACTS 编辑通讯录	允许 App 写入用户通讯录
9		GET_ACCOUNTS 获取 App 账户	允许 App 从账户服务中获取 App 账户列表
10	LOCATION 位置	ACCESS_FINE_LOCATION 访问精准定位	允许 App 获取基于 GPS 等的精准地理位置
11		ACCESS_COARSE_LOCATION 访问粗略位置	允许 App 获取基于基站、IP 等分析得到的粗略地理位置
12		ACCESS_BACKGROUND_LOCATION 支持后台访问位置	允许 App 在后台运行时使用位置信息（需要 App 获得访问粗略位置或访问精准位置权限）
13	MICROPHONE 麦克风	RECORD_AUDIO 录音	允许 App 使用麦克风进行录音

序号	权限分组	权限名	权限功能描述
14	PHONE 电话	READ_PHONE_STATE 读取设备信息	App 可通过此权限获取设备 IMSI（国际移动用户识别码）、IMEI（国际移动设备识别码）等设备唯一标识信息，以及手机通话状态等
15		READ_PHONE_NUMBERS 读取本机电话号码	允许 App 读取用户的本机电话号码
16		CALL_PHONE 拨打电话	允许 App 直接拨打电话
17		ANSWER_PHONE_CALLS 接听电话	允许 App 接听拨入的电话
18		ADD_VOICEMAIL 添加语音邮件	允许 App 向邮件中添加语音附件
19		USE_SIP 使用网络电话	允许 App 拨打/接听 SIP 网络电话
20		ACCEPT_HANDOVER 允许切换通话	允许 App 继续进行在其他 App 中发起的通话
21	SENSORS 传感器	BODY_SENSORS 获取身体传感器信息	允许 App 访问身体内部状况相关的传感器数据，一般特指心率传感器数据
22	SMS 短信	SEND_SMS 发送短信	允许 App 发送短信
23		RECEIVE_SMS 接收短信	允许 App 接收短信
24		READ_SMS 读取文字讯息（短信或彩信）	允许 App 读取短信或彩信
25		RECEIVE_WAP_PUSH 接收 WAP 推送	允许 App 接收 WAP 推送信息
26		RECEIVE_MMS 接收彩信	允许 App 接收彩信
27	STORAGE 存储	READ_EXTERNAL_STORAGE 读取公共存储区	允许 App 读取公共存储区
28		WRITE_EXTERNAL_STORAGE 写入公共存储区	允许 App 写入公共存储区

序号	权限分组	权限名	权限功能描述
29		ACCESS_MEDIA_LOCATION 读取照片位置信息	允许 App 读取照片文件中包含的拍摄地点信息
30	ACTIVITY_RECOGNITION 身体活动	ACTIVITY_RECOGNITION 识别身体活动	允许 App 获取身体活动相关信息，如未移动、步行、跑步、骑行、在车辆中等

注：支持后台访问位置（ACCESS_BACKGROUND_LOCATION）、读取照片位置信息（ACCESS_MEDIA_LOCATION）、识别身体活动（ACTIVITY_RECOGNITION）为安卓10中新增权限；监控呼出电话（PROCESS_OUTGOING_CALLS）已在安卓10中废弃。

ios 系统权限名称命名及功能描述参考示例见表 A.2。

表 A.2 ios 系统权限名称命名及功能描述参考示例

序号	权限分组	权限名	权限功能描述
1	Calendar and Reminders 日历与提醒事项	Calendars 日历	访问用户日历数据
2		Reminders 提醒事项	访问用户提醒事项
3	Camera and Microphone 相机与麦克风	Camera 相机	访问设备的相机
4		Microphone 麦克风	访问设备的麦克风
5	Contacts 通讯录	Contacts 通讯录	访问用户的联系人
6	Health 健康	Health Records 健康记录	读取临床健康记录
7		Health Share 读取 HealthKit 健康数据	从 HealthKit 存储读取样本
8		Health Update 更新 HealthKit 健康数据	将样本保存到 HealthKit 存储
9	Location 定位服务	Location Always and When In Use 始终访问位置	始终访问用户的位置信息
10		Location 访问位置	访问用户的位置信息
11		Location When In Use 使用期间访问位置	使用 App 期间（前台运行时）访问用户的位置信息
12	MediaPlayer 媒体与 Apple Music	Media Library 媒体库	访问用户的媒体库
13	Motion 运动与健身	Motion 运动与健身	访问设备的加速度计
14	Photos 照片	Photo Library Additions 只写照片库	只写访问用户照片库
15		Photo Library 读取和写入照片库	读取和写入用户照片库

鸿蒙系统权限名称命名及功能描述参考示例见表 A.3。

表 A.3 鸿蒙系统权限名称命名及功能描述参考示例

序号	权限分组	权限名	权限功能描述
1	CALENDAR 日历	READ_CALENDAR 读取日历	允许 App 读取用户日历数据
2		WRITE_CALENDAR 编辑日历	允许 App 写入用户日历数据
3	CAMERA 相机	CAMERA 拍摄	允许应用使用相机拍摄照片和录制视频
4	MICROPHONE 麦克风	MICROPHONE 录音	允许应用使用麦克风进行录音
5	LOCATION 位置	LOCATION 访问前台定位	允许应用在前台运行时获取位置信息。
6		LOCATION_IN_BACKGROUND 访问后台定位	允许应用在后台运行时获取位置信息，需要同时申请 LOCATION 权限
7	MOTION 健身运动	ACTIVITY_MOTION 健身运动	允许应用读取用户当前的运动状态
8	HEALTH 健康	READ_HEALTH_DATA 健康	允许应用读取用户的健康数据
9	MEDIA 媒体	MEDIA_LOCATION 读取媒体位置信息	允许应用访问用户媒体文件中的地理位置信息
10		READ_MEDIA 读取媒体文件	允许应用读取用户外部存储中的媒体文件信息
11		WRITE_MEDIA 读写媒体文件	允许应用读写用户外部存储中的媒体文件信息

附 录 B
（资料性）
移动智能终端敏感数据管理参考示例

移动智能终端敏感数据/能力管理参考示例见表 B.1。

表 B.1 敏感数据/能力管理参考示例

敏感数据/能力	功能描述	是否提示	是否记录	通过权限实现授权粒度
应用程序列表	获取所有已安装 App 的信息，例如已安装应用程序的名称、包名、版本等。	否	是	始终允许、拒绝
位置信息	获取经纬度	是	是	始终允许、拒绝、每次使用询问、仅使用期间允许
	注册监听函数	否	否	
	获取粗略经纬度	是	是	
剪切板	操作系统提供的用于共享的缓存数据模块	是	否	—
屏幕截图	通过截图方式获取移动智能终端屏幕显示的快照或图片	否	否	—
相机	实现拍照、摄像、扫描等功能	是	是	拒绝、每次使用询问、仅使用期间允许
麦克风	实现语音通话等功能	是	是	拒绝、每次使用询问、仅使用期间允许

参 考 文 献

[1] GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南

[2] GB/T 41391—2022 信息安全技术 移动互联网应用程序（App）收集个人信息基本要求

[3] TC260-PG-20191A 网络安全实践指南—移动互联网应用基本业务功能必要信息规范

[4] TC260-PG-20202A 网络安全标准实践指南—移动互联网应用程序（App）收集使用个人信息自评估指南

[5] TC260-PG-20203A 网络安全标准实践指南—移动互联网应用程序（App）个人信息保护常见问题及处置指南

[6] TC260-PG-20204A 网络安全标准实践指南—移动互联网应用程序（App）系统权限申请使用指南

[7] TC260-PG-20205A 网络安全标准实践指南—移动互联网应用程序（App）使用软件开发工具包（SDK）安全指引

[8] 常见类型移动互联网应用程序必要个人信息范围规定〔2021 年 3 月 22 日国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局发布〕

[9] App 违法违规收集使用个人信息行为认定方法（2019 年 12 月 30 日国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局发布）

[10] 工业和信息化部关于开展纵深推进 App 侵害用户权益专项整治行动的通知〔工信部信管函〔2020〕164 号〕