电 信 终 端 产 业 协 会 标 准

TAF-WG4-AS0051-V1.0.0:2019

移动智能终端及应用软件用户个人信息保护实施指南

第 5 部分：终端权限管理

Mobile Intelligent Terminal and Application Software User Personal Information Protection Implementation Guide

Part 5: Permission Management of Terminal

2019-12-26 发布　　2019-12-26 实施

电信终端产业协会　　发 布

目 次

前　　言

本标准按照 GB/T 1.1-2009给出的规则起草。

本标准由电信终端产业协会提出并归口。

本标准起草单位：OPPO广东移动通信有限公司、中国信息通信研究院、华为技术有限公司、维沃移动通信有限公司、北京三星通信技术研究有限公司、北京奇虎科技有限公司

本标准主要起草人：邹海荣、詹维骁、李腾、董雯、宁华、衣强、王江胜、贾科、吴春雨、姚一楠、赵晓娜

引　　言

手机等移动智能终端设备的爆发式增长，以及移动互联网的发展使得手机成为了日常生活不可或缺的一部分，使用时长的不断增加使得手机等移动智能终端设备上存储着大量用户个人信息与敏感信息。因此，手机等智能移动终端设备成为了隐私窃取的新热点。随着手机功能的增强，价值越来越大，与之相伴的是越来越严峻的安全挑战。

在众多的移动平台中，Android平台以其开放性和良好的生态环境受到广大的手机厂商和用户的青睐。 然而，Android应用生态的安全情况并不容乐观：例如，Android系统权限项目繁多，不便于用户理解与管理，在应用申请权限时往往一概授予；又如，权限管理往往“非黑即白”，一旦对应用授予某项权限，则该应用可以随时使用，缺少使用时询问或提示；再如，Android系统的开放性也导致对APP缺少必要的约束，APP过度获取非必要权限，以及不授权不能使用功能的“霸王条款”等情况较为普遍。

移动智能终端权限管理的效果直接决定了应用是否可以读取到用户的个人信息。所以，出于对用户个人信息保护的需要，终端权限管理标准迫切需要出台。这不仅涉及移动智能终端的规范，更是用户个人信息安全的话题。本标准将适用于可安装由第三方开发者开发的应用软件的移动智能终端，为移动智能终端厂商及终端设备应用开发者提供权限管理设计依据。

移动智能终端及应用软件用户个人信息保护实施指南 第5部分：终端权限管理

1 范围

本标准规定了移动智能终端权限管理的要求，包括移动智能终端权限范围定义；移动智能终端权限分类与分级；移动智能终端权限管理显示规范；移动智能终端权限申请方式、授予方式与撤销方式；移动智能终端权限提示等。

本标准适用于各种制式的移动智能终端（主要针对搭载了Android系统的移动智能终端），个别条款不适用于特殊行业、专业应用，其他终端也可参考使用。

2 术语、定义

本标准术语和定义引用《移动智能终端与应用软件用户个人信息保护实施指南 第1部分：总则》。

3 移动智能终端权限分级

应用软件在移动智能终端上运行时，在默认情况下都没有权限执行对其他应用、操作系统或用户有不利影响的任何操作。包括读取或写入用户的个人信息（例如联系人、电子邮件、日历等）、读取或写入其他应用软件的文件、执行网络访问、使设备保持唤醒状态等。

应用软件需要使用的权限可以分为两大类：访问个人信息，使用特定的系统功能。按照不同的保护等级要求，操作系统可以提醒用户授权，或者自动授予应用相关权限。

根据应用软件获取对应权限后对用户的个人信息、操作系统或用户造成的风险程度，对移动智能终端权限等级划分为：一般权限、敏感权限、核心敏感权限、特殊权限以及厂商自定义权限。

3.1 一般权限

一般权限涵盖了应用软件需要访问应用软件沙箱外部数据或资源的区域，但对用户个人信息或其他应用软件风险非常小的操作。 例如，设置时区的权限是一般权限。

如果应用软件在其清单中声明它需要一般权限，则操作系统会在安装时自动授予应用软件该权限。操作系统不会提示用户授予一般权限，用户也无法撤消这些权限。一般权限包括但不限于以下权限：

权限名称	权限描述
访问额外位置(ACCESS_LOCATION_EXTRA_COMMANDS)	允许应用软件访问额外的位置提供指令
获取网络连接(ACCESS_NETWORK_STATE)	允许获取网络连接信息
设置通知(ACCESS_NOTIFICATION_POLICY)	允许设置通知策略
蓝牙(BLUETOOTH)	允许应用软件连接配对过的蓝牙设备

管理蓝牙(BLUETOOTH_ADMIN)	允许应用软件管理蓝牙，搜索和配对新的蓝牙设备
发送持久广播(BROADCAST_STICKY)	允许应用发送持久广播
更改网络连接状态(CHANGE_NETWORK_STATE)	允许应用更改网络连接状态，自动切换网络
改变WIFI多播模式(CHANGE_WIFI_MULTICAST_STATE)	允许应用进入WIFI多播模式，允许应用使多播地址接收发送到无线网络上所有设备（而不仅是用户手机）数据包。
更改WIFI连接状态(CHANGE_WIFI_STATE)	允许应用改变WIFI连接状态
禁用锁屏(DISABLE_KEYGUARD)	允许应用禁用系统锁屏。允许应用停用键锁以及任何关联的密码安全措施。例如让手机在接听来电时停用键锁，在通话结束后重新启用键锁。
展开或折叠状态栏(EXPAND_STATUS_BAR)	允许应用展开和折叠状态栏
前台服务(FOREGROUND_SERVICE)	允许应用使用前台服务
获取包大小(GET_PACKAGE_SIZE)	允许应用获取安装包占空间大小
安装桌面快捷方式(INSTALL_SHORTCUT)	允许应用在桌面安装快捷方式
使用互联网(INTERNET)	允许应用打开网络接口
后台杀进程(KILL_BACKGROUND_PROCESSES)	允许应用调用特定方法结束其他应用的后台进程
管理自身通话(MANAGE_OWN_CALLS)	允许拥有通话功能的应用通过自身连接管理服务接口处理自身的通话行为
修改音频设置(MODIFY_AUDIO_SETTINGS)	允许该应用修改移动智能终端音频设置
使用NFC(NFC)	允许应用使用NFC进行I/O操作，与其他NFC标签、卡和读卡器通信
读取帐户同步设置(READ_SYNC_SETTINGS)	允许该应用读取某个帐户的同步设置。例如，此权限可确定“联系人”是否与允许该应用读取某个帐户的同步设置
读取帐户同步统计信息(READ_SYNC_STATS)	允许该应用读取某个帐户的同步统计信息，包括活动历史记录和数据量
接收启动完成广播(RECEIVE_BOOT_COMPLETED)	允许应用接收系统启动完成广播
重新排序正在运行的应用(REORDER_TASKS)	允许应用对正在运行的应用重新排序
请求后台运行(REQUEST_COMPANION_RUN_IN_BACKGROUND)	允许应用在后台运行
请求后台使用数据(REQUEST_COMPANION_USE_DATA_IN_BACKGROUND)	允许应用在后台使用数据

请求卸载应用(REQUEST_DELETE_PACKAGES)	允许应用卸载其他应用
忽略电池优化策略(REQUEST_IGNORE_BATTERY_OPTIMIZATIONS)	允许应用忽略系统电池优化策略
设置闹钟(SET_ALARM)	允许应用设置闹钟
设置时区(SET_TIME_ZONE)	允许应用设置系统时区
设置壁纸(SET_WALLPAPER)	允许应用设置系统壁纸
设置壁纸提示(SET_WALLPAPER_HINTS)	允许应用设置有关系统壁纸大小的提示
使用红外线发射器(TRANSMIT_IR)	允许应用使手机的红外线发射器
删除桌面快捷方式(UNINSTALL_SHORTCUT)	允许应用删除桌面快捷方式
使用指纹(USE_FINGERPRINT)	允许应用使手机指纹设备
振动(VIBRATE)	允许应用使手机振动
唤醒锁(WAKE_LOCK)	允许应用持有系统唤醒锁，防止进程进入睡眠状态或息屏
修改帐户同步设置(WRITE_SYNC_SETTINGS)	允许该应用修改某个帐户的同步设置，包括启用和停用同步

备注：“一般权限”对应Android操作系统中对应权限级别为“normal”的权限，如当前移动终端搭载的操作系统为Android操作系统，且上述权限中未提及的“normal”级别的权限，可按一般权限处理。

3.2 敏感权限

敏感权限涵盖应用软件需要涉及用户个人敏感信息的数据或资源的区域，或者可能会影响用户存储的数据或其他应用软件的操作。 例如，读取设备识别码（IMEI、Wi-Fi MAC地址等）的权限是一种敏感权限。 如果应用软件声明它需要敏感权限，则操作系统必须让用户明确授予该应用软件的权限。 在用户授予该权限之前，操作系统应确保应用软件无法提供依赖该权限的功能。敏感权限包括但不限于以下权限：

权限名称	权限描述
读取日历(READ_CALENDAR)	读取日历内容
写入或删除日历(WRITE_CALENDAR)	修改日历内容
读取手机识别码(READ_PHONE_STATE)	允许应用软件读取电话状态
读取联系人(READ_CONTACTS)	允许应用软件读取联系人通讯录信息
写入或删除联系人(WRITE_CONTACTS)	允许应用软件写入联系人，但不可读取
访问手机账户列表(GET_ACCOUNTS)	允许应用软件访问当前手机的账户列表信息
读取传感器(BODY_SENSORS)	允许应用软件访问用户用来衡量身体内发生的情况的传感器的数据，例如心率
发送短信(SEND_SMS)	允许应用软件发送短信
接收短信(RECEIVE_SMS)	允许应用软件接收短信
读取短信(READ_SMS)	允许应用软件读取短信内容

接收WAP PUSH(RECEIVE_WAP_PUSH)	允许应用软件接收WAP PUSH信息
接收彩信(RECEIVE_MMS)	允许应用软件接收彩信
读取外部存储空间(READ_EXTERNAL_STORAGE)	允许应用软件读取扩展存
写入外部存储空间(WRITE_EXTERNAL_STORAGE)	允许应用软件写入外部存储，如SD卡上写文件
获取无线状态(ACCESS_WIFI_STATE)	允许获取无线网络相关信息

备注：

1.“敏感权限”对应Android操作系统中对应权限级别为“dangerous”的权限，如当前移动终端搭载的操作系统为Android操作系统，且上述权限及下文“核心敏感权限”中均未提及的“dangerous”级别的权限，须按敏感权限处理。

2.“获取无线状态”权限为建议项，也可归为一般权限管理。

3.3 核心敏感权限

核心敏感权限涵盖应用软件需要涉及用户个人敏感信息的数据或资源的区域，或者可能会影响用户存储的数据或其他应用软件的操作。通过核心敏感权限，可精准获得用户的个人敏感信息。 例如，使用摄像头的权限是一种核心敏感权限。 如果应用软件声明它需要敏感权限，则操作系统必须让用户明确授予该应用软件的权限。在用户授予该权限之前，操作系统应确保应用软件无法提供依赖该权限的功能。核心敏感权限被授予后，应用软件在使用核心敏感权限过程中操作系统仍可适当增加显性的实时提示告知用户核心敏感权限正在被使用。核心敏感权限包括但不限于以下权限：

权限名称	权限描述
使用摄像头(CAMERA)	允许应用软件调用设备的摄像头进行拍摄、录像
访问精确位置(ACCESS_FINE_LOCATION)	允许应用软件通过GPS获取精确的位置信息
访问大致位置(ACCESS_COARSE_LOCATION)	允许应用软件通过WiFi或移动基站获取粗略的位置信息
录音或通话录音(RECORD_AUDIO)	允许应用获取麦克风输入数据信息
使用SIP(USE_SIP)	允许应用软件使用SIP视频服务
拨打电话(CALL_PHONE)	允许应用软件拨打电话，从非系统拨号器里初始化一个电话拨号
读取通话记录(READ_CALL_LOG)	允许应用软件读取通话记录
写入通话记录(WRITE_CALL_LOG)	允许应用软件写入通话记录
使用语音邮件(ADD_VOICEMAIL)	允许应用软件使用语音邮件
修改外拨电话(PROCESS_OUTGOING_CALLS)	允许应用软件监视、修改外拨电话

3.4 特殊权限

特殊权限指会对个人敏感信息、用户体验、其他应用安全、设备安全、系统稳定造成极大损害的权限。应用软件在申请特殊权限时，操作系统不能以便捷的方式让用户授予，应通过向用户显示详细的管理界面来响应应用软件的意图，可适当增加障碍设计，避免用户误操作开启特殊权限。特殊权限授权后，应用软件在使用核心敏感权限过程中操作系统仍可适当增加显性的实时提示及提供快捷的撤销授权方式。特殊权限包括但不限于以下权限：

权限名称	权限描述
设备管理器(BIND_DEVICE_ADMIN)	激活使用设备管理器

辅助模式(BIND_ACCESSIBILITY_SERVICE)	使用无障碍功能
读写系统设置(WRITE_SETTINGS)	允许应用读取或写入系统设置
读取应用通知(BIND_NOTIFICATION_LISTENER_SERVICE)	允许应用读取应用的通知内容
悬浮窗(SYSTEM_ALERT_WINDOW)	允许应用显示在其他应用之上，或后台弹出界面
读取应用使用情况(PACKAGE_USAGE_STATS)	允许应用读取本机的应用使用情况
请求安装应用(REQUEST_INSTALL_PACKAGES)	允许应用安装其他应用

3.5 终端设备厂商自定义权限

终端设备厂商自定义权限（以下简称“自定义权限”）指由终端设备厂商根据自身研发实力及市场洞察，为了保护用户个人信息、用户体验、设备安全，维持系统稳定而自定义的权限。终端设备厂商对于自定义权限可自行设计授权、管控方式，自定义权限可包含一般权限。例如以下权限：

权限名称	权限描述
自启动	应用可自启动，允许应用始终运行
关联启动	允许应用被其他应用拉起，即使用户没有主动使用
使用WLAN	使用无线网络连接
使用移动数据	使用移动数据网络
截取屏幕或录制屏幕	截取屏幕或录制屏幕

4 移动智能终端权限分组

4.1 分组目的

操作系统在应用软件申请敏感权限、核心敏感权限时需要明示用户，如逐一确认，明示过程冗长繁琐，增加用户的使用负担，用户体验差。所以对于敏感权限、核心敏感权限可进行分组，同一分组的敏感权限、核心敏感权限可一次性全部申请允许、禁止。

用户也可对权限组中的单项权限进行单独控制，控制选项应包含允许、禁止，建议增加询问选项。

4.2 权限分组

移动智能终端操作系统在权限分组时，可参考附录B中的分组。

5 移动智能终端权限管理

5.1 概述

为方便用户使用、理解移动智能终端权限，移动智能终端权限管理应至少支持以应用软件维度进行管理，可增加以权限维度管理。用户可根据实际场景需要，使用不同的管理方式。敏感权限、核心敏感权限需要采用此种方式，一般权限可以参考，不做限制。特殊权限、自定义权限由终端设备厂商自行决定，不做要求。

5.2 以权限维度管理

以权限维度管理时，以权限名称为管理单元，列举所有当前移动智能终端使用到此权限的应用软件，统一展示、管理，并明示该权限对所有用到此权限的授予情况。展示方式可参考附录B中的权限分组规则。

5.3 以应用软件维度管理

以应用软件维度管理时，以应用软件名称为管理单元，列举该应用软件所用到的所有权限，统一展示、管理，并明示所有权限的授予情况。展示方式可参考附录B中的权限分组规则。

6 移动智能终端敏感权限及核心敏感权限申请、授予与撤销

6.1 概述

应用软件在申请使用敏感权限、核心敏感权限时，需要获得用户允许，操作系统必须以显性的方式提示用户。

6.2 终端权限管控安全能力

应用软件在权限被授予前，权限覆盖范围下的数据或接口，操作系统需要提供安全防护能力，未被授权的应用软件无法获取对应权限覆盖范围下的数据或调用相应接口。

6.3 终端权限申请要求

应用软件在需要使用权限时，需向操作系统发起申请，操作系统以显性的方式提示用户，方式可以为弹框、通知、浮窗等。需要用户主动确认同意授予后才可继续执行相应操作。敏感权限、核心敏感权限申请时，需要描述权限组及权限组下对应的子权限。

预置应用可单次申请所有敏感权限、核心敏感权限，描述所需权限的及具体用途。非预置应用操作系统需要提供用户可逐一授权的交互方式。

6.4 终端权限授予要求

权限授予可分为：允许、禁止、询问，用户可自由选择。授予权限组后，该权限组下的所有权限都授予。

6.5 终端权限撤销要求

已授予的权限可撤销授予，用户可在权限管理界面针对单独应用软件进行撤销权限授予操作，可修改为禁止或询问。撤销权限组授权后，该权限组下的所有子权限都撤销授权。

7 分发平台对非预置应用权限声明要求

分发平台应要求平台的非预置应用在上架时注明所需的所有敏感权限、核心敏感权限，并明示具体用途。

8 权限管理配置管理建议

终端设备厂商可针对非预置应用给出权限配置建议，对于新安装的非预置应用配置推荐的权限配置，以减少用户的使用负担。推荐配置前需要用户明确授权，用户未授权前不能进行推荐行为。用户可覆盖修改厂商默认的推荐设置。终端设备厂商可根据新安装应用向系统请求多项权限时进行合并展示，允许用户进行单项或多项授权（如附录C中示例）。

附 录 A
（规范性附录）
标准修订历史

修订时间	修订后版本号	修订内容

附 录 B
（资料性附录）
Android P 系统权限列表

ACCEPT_HANDOVER
ACCESS_CHECKIN_PROPERTIES
ACCESS_COARSE_LOCATION
ACCESS_FINE_LOCATION
ACCESS_LOCATION_EXTRA_COMMANDS
ACCESS_NETWORK_STATE
ACCESS_NOTIFICATION_POLICY
ACCESS_WIFI_STATE
ACCOUNT_MANAGER
ADD_VOICEMAIL
ANSWER_PHONE_CALLS
BATTERY_STATS
BIND_ACCESSIBILITY_SERVICE
BIND_APPWIDGET
BIND_AUTOFILL_SERVICE
BIND_CARRIER_MESSAGING_SERVICE
BIND_CARRIER_SERVICES
BIND_CHOOSER_TARGET_SERVICE

BIND_CONDITION_PROVIDER_SERVICE
BIND_DEVICE_ADMIN
BIND_DREAM_SERVICE
BIND_INCALL_SERVICE
BIND_INPUT_METHOD
BIND_MIDI_DEVICE_SERVICE
BIND_NFC_SERVICE
BIND_NOTIFICATION_LISTENER_SERVICE
BIND_PRINT_SERVICE
BIND_QUICK_SETTINGS_TILE
BIND_REMOTEVIEWS
BIND_SCREENING_SERVICE
BIND_TELECOM_CONNECTION_SERVICE
BIND_TEXT_SERVICE
BIND_TV_INPUT
BIND_VISUAL_VOICEMAIL_SERVICE
BIND_VOICE_INTERACTION
BIND_VPN_SERVICE
BIND_VR_LISTENER_SERVICE
BIND_WALLPAPER
BLUETOOTH

BLUETOOTH_ADMIN
BLUETOOTH_PRIVILEGED
BODY_SENSORS
BROADCAST_PACKAGE_REMOVED
BROADCAST_SMS
BROADCAST_STICKY
BROADCAST_WAP_PUSH
CALL_PHONE
CALL_PRIVILEGED
CAMERA
CAPTURE_AUDIO_OUTPUT
CAPTURE_SECURE_VIDEO_OUTPUT
CAPTURE_VIDEO_OUTPUT
CHANGE_COMPONENT_ENABLED_STATE
CHANGE_CONFIGURATION
CHANGE_NETWORK_STATE
CHANGE_WIFI_MULTICAST_STATE
CHANGE_WIFI_STATE
CLEAR_APP_CACHE
CONTROL_LOCATION_UPDATES
DELETE_CACHE_FILES

DELETE_PACKAGES
DIAGNOSTIC
DISABLE_KEYGUARD
DUMP
EXPAND_STATUS_BAR
FACTORY_TEST
FOREGROUND_SERVICE
GET_ACCOUNTS
GET_ACCOUNTS_PRIVILEGED
GET_PACKAGE_SIZE
GET_TASKS
GLOBAL_SEARCH
INSTALL_LOCATION_PROVIDER
INSTALL_PACKAGES
INSTALL_SHORTCUT
INSTANT_APP_FOREGROUND_SERVICE
INTERNET
KILL_BACKGROUND_PROCESSES
LOCATION_HARDWARE
MANAGE_DOCUMENTS
MANAGE_OWN_CALLS

MASTER_CLEAR
MEDIA_CONTENT_CONTROL
MODIFY_AUDIO_SETTINGS
MODIFY_PHONE_STATE
MOUNT_FORMAT_FILESYSTEMS
MOUNT_UNMOUNT_FILESYSTEMS
NFC
NFC_TRANSACTION_EVENT
PACKAGE_USAGE_STATS
PERSISTENT_ACTIVITY
PROCESS_OUTGOING_CALLS
READ_CALENDAR
READ_CALL_LOG
READ_CONTACTS
READ_EXTERNAL_STORAGE
READ_FRAME_BUFFER
READ_INPUT_STATE
READ_LOGS
READ_PHONE_NUMBERS
READ_PHONE_STATE
READ_SMS

READ_SYNC_SETTINGS
READ_SYNC_STATS
READ_VOICEMAIL
REBOOT
RECEIVE_BOOT_COMPLETED
RECEIVE_MMS
RECEIVE_SMS
RECEIVE_WAP_PUSH
RECORD_AUDIO
REORDER_TASKS
REQUEST_COMPANION_RUN_IN_BACKGROUND
REQUEST_COMPANION_USE_DATA_IN_BACKGROUND
REQUEST_DELETE_PACKAGES
REQUEST_IGNORE_BATTERY_OPTIMIZATIONS
REQUEST_INSTALL_PACKAGES
RESTART_PACKAGES
SEND_RESPOND_VIA_MESSAGE
SEND_SMS
SET_ALARM
SET_ALWAYS_FINISH
SET_ANIMATION_SCALE

SET_DEBUG_APP
SET_PREFERRED_APPLICATIONS
SET_PROCESS_LIMIT
SET_TIME
SET_TIME_ZONE
SET_WALLPAPER
SET_WALLPAPER_HINTS
SIGNAL_PERSISTENT_PROCESSES
STATUS_BAR
SYSTEM_ALERT_WINDOW
TRANSMIT_IR
UNINSTALL_SHORTCUT
UPDATE_DEVICE_STATS
USE_BIOMETRIC
USE_FINGERPRINT
USE_SIP
VIBRATE
WAKE_LOCK
WRITE_APN_SETTINGS
WRITE_CALENDAR
WRITE_CALL_LOG

WRITE_CONTACTS
WRITE_EXTERNAL_STORAGE
WRITE_GSERVICES
WRITE_SECURE_SETTINGS
WRITE_SETTINGS
WRITE_SYNC_SETTINGS
WRITE_VOICEMAIL

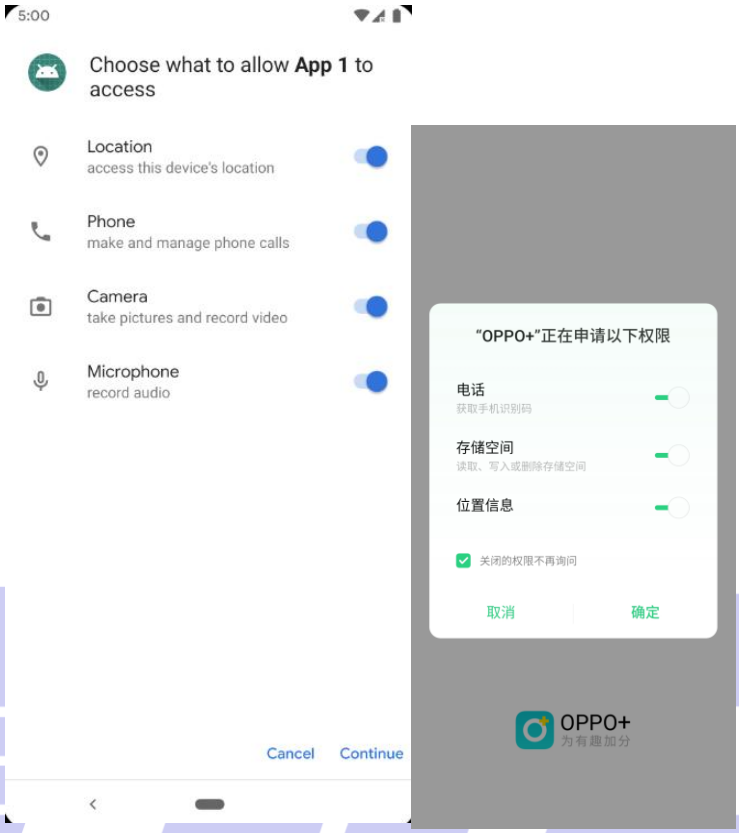
备注：此附录的权限参考的是Android P版本，如与当前移动终端搭载的操作系统版本不同，以搭载的操作系统版本对应的Android官方权限列表为准。

Android P 系统权限组及对应权限

附　录　APermission group	Permission
CALENDAR	READ_CALENDAR
	WRITE_CALENDAR
CALL_LOG	READ_CALL_LOG
	WRITE_CALL_LOG
	PROCESS_OUTGOING_CALLS
CAMERA	CAMERA
CONTACTS	READ_CONTACTS
	WRITE_CONTACTS
	GET_ACCOUNTS
LOCATION	ACCESS_FINE_LOCATION
	ACCESS_COARSE_LOCATION
MICROPHONE	RECORD_AUDIO
PHONE	READ_PHONE_STATE
	READ_PHONE_NUMBERS
	CALL_PHONE
	ANSWER_PHONE_CALLS
	ADD_VOICEMAIL
	USE_SIP
SENSORS	BODY_SENSORS
SMS	SEND_SMS
	RECEIVE_SMS
	READ_SMS
	RECIEVE_WAP_PUSH
	RECIEVE_MMS
STORAGE	READ_EXTERNAL_STORAGE
	WRITE_EXTERNAL_STORAGE

备注：此附录的权限参考的是Android P版本，如与当前移动终端搭载的操作系统版本不同，以搭载的操作系统版本对应的Android官方权限分组为准

新安装应用启动多项授权申请时系统进行合并展示的方式



参 考 文 献