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

（v1.0-202009）

全国信息安全标准化技术委员会秘书处

2020 年 9 月

本文档可从以下网址获得：

www.tc260.org.cn/

全国信息安全标准化技术委员会

NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国信息安全标准化技术委员会（以下简称“信安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

声　明

本《实践指南》版权属于信安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《实践指南》的任何部分。凡转载或引用本《实践指南》的观点、数据，请注明“来源：全国信息安全标准化技术委员会秘书处”。

技术支持单位

本《实践指南》得到中国电子技术标准化研究院、华为技术有限公司、清华大学、小米科技有限责任公司、阿里巴巴（北京）软件服务有限公司、三六零科技集团有限公司、中国移动通信集团有限公司、北京京东尚科信息技术有限公司、京东数字科技控股有限公司、上海钧正网络科技有限公司、浙江蚂蚁小微金融服务集团股份有限公司、北京三快科技有限公司、深圳市腾讯计算机系统有限公司、北京百度网讯科技有限公司、浙江每日互动网络科技股份有限公司、北京字节跳动科技有限公司、北京小桔科技有限公司等单位的技术支持。

摘　要

本实践指南依据法律法规和政策标准要求，针对App申请使用系统权限存在的强制、频繁、过度索权，及捆绑授权、私自调用权限上传个人信息、敏感权限滥用等典型问题，给出了App申请使用系统权限的基本原则和安全要求，建议App提供者参考本实践指南规范App系统权限申请和使用行为，防范因系统权限不当利用造成的个人信息安全风险。

目 录

1 范围

本实践指南给出了移动互联网应用程序（App）申请、使用系统权限的基本原则和通用要求，以及通讯录、短信、通话记录、位置等10类安卓系统典型权限的申请使用要求[1]。

本实践指南适用于App提供者规范系统权限申请和使用行为，也可为App开发者、移动互联网应用分发平台运营者和移动智能终端厂商提供参考。

2 术语定义

2.1 移动互联网应用程序

通过预装、下载等方式获取并运行在移动智能终端上、向用户提供服务的应用软件，简称App。

注：本实践指南中的App不包括移动智能终端操作系统基本组件应用。

2.2 移动互联网应用程序提供者

移动互联网应用程序所有者或运营者，简称App提供者。

2.3 可收集个人信息权限

移动智能终端操作系统向App开放的，具有收集个人信息能力的系统权限，简称系统权限或权限，范围可参考附录A。

2.4 权限申请

向移动智能终端操作系统声明，并向用户请求授权，以获得对移动智能终端数据或能力的访问许可的过程。

[1] 本实践指南主要针对安卓和iOS的系统权限，全文内容均适用于安卓，第二章、第三章、第四章、附录A和附录C适用于iOS。

3 权限申请的原则和要求

3.1 权限申请基本原则

a) 最小必要原则：仅申请 App 业务功能所必需的权限，不申请与 App 业务功能无关的权限。

b) 用户可知原则：申请的权限均应有明确、合理的使用场景，并告知用户权限申请目的。

c) 不强制不捆绑原则：不应强制申请系统权限，不要求用户一次性授权同意打开多个系统权限。

d) 动态申请原则：App 所需的权限应在对应业务功能执行时动态申请。在用户未触发相关业务功能时，不提前申请与当前业务功能无关的权限。

3.2 权限申请通用要求

a) 权限申请应满足“最小必要”原则，与业务功能无关的系统权限不向操作系统声明，例如无关的安卓系统权限不在AndroidManifest.xml文件中声明。

注 1：附录 A 中表 A.1 的“业务功能示例”给出了与权限相关的业务功能示例。

注 2：附录 D 给出了与常见服务类型相关程度较低，不建议申请的安卓系统权限。

b) 申请权限时应同步告知权限申请目的，目的应明确且易于理解，不包含广告及任何欺诈、诱骗、误导用户授权的描述。

c) App（包括嵌入的SDK）申请所需权限，应在声明文件（如AndroidManifest.xml）中严格按照格式规范逐个声明。

d) 如仅需使用权限组中部分权限，不应在权限声明文件中声明同一权限组其他权限，例如当App仅需使用写入日历权限时，不应在

AndroidManifest.xml中声明读取日历权限。

e) 如用户拒绝或撤回授予某服务类型非必要系统权限，App不应强制退出或关闭，且不影响与此权限无关的业务功能使用。

注：服务类型的必要系统权限，可参考《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范》的常见服务类型最小必要个人信息进行判断。

f) 如用户明确拒绝App业务功能所需权限，App不应频繁申请系统权限干扰用户正常使用，除非由用户主动触发功能，且没有该权限参与此业务功能无法实现。“频繁”的形式包括但不限于：

1) 单个场景在用户拒绝权限后，48小时内弹窗提示用户打开系统权限的次数超过1次；

2) 每次重新打开App或使用某一业务功能时，都会向用户索要或提示用户缺少相关系统权限。

g) 除仅用于安全风控场景外，App不应收集不可变更的唯一设备识别码（如IMEI、MAC地址）。

h) 定向推送和用户画像场景下标识用户时，应使用可重置的标识符，且标识符不与可识别用户身份信息或不可变更的唯一设备识别码关联。

i) 如App业务功能所需的权限被用户拒绝且选择禁止后不再提示，当用户再次使用此功能时，宜以不干扰用户的方式（如文字提示）引导用户到系统设置中去开启所需权限。

j) App应尊重用户的权限设置，不应欺骗或强迫用户同意不必要的数据访问，若有可能宜为拒绝授权的用户提供替代解决方案。

注：例如如果非导航场景下用户拒绝位置权限，可提供手动输入地址的功能。

k) 内嵌第三方SDK的App，宜要求SDK向App明示申请的系统权限及申请目的。

l) App宜对内嵌第三方SDK申请使用权限进行审核，确保其申请的权限有业务功能场景对应，且不超过约定的范围。

4 权限使用的原则和要求

4.1 权限使用基本原则

a) 一致性原则：权限的使用应与权限申请时和隐私政策中所描述的目的用途、使用场景和规则相一致。

b) 不扩散原则：App 通过系统权限获得的数据和能力，不应在用户未授权的情况下私自提供给小程序或终端上的其他 App 使用。

c) 访问显性化原则：使用系统权限（例如相机、麦克风、位置）获取个人敏感信息时，应采用显性方式提示用户，避免以隐蔽方式收集用户个人信息。

4.2 权限使用通用要求

a) 权限申请获得授权后，App应仅访问满足业务功能需要的最少个人信息，例如读取日历时，若仅需读取某个日期的日程信息则不应读取其他日期的日程。

b) 权限申请后自动采集个人信息的频率应在实现App业务功能所必需的最低合理频率范围内。

c) App不应未经用户同意更改其设置的系统权限授权状态，如App更新时自动将用户设置的权限恢复到默认状态。

d) 若系统权限申请目的、使用场景发生变化，应重新告知用户。

e) 当App对外提供的接口涉及个人信息，且操作系统定义的权限无法达到目的时，App应通过自定义权限对访问个人信息的对外交互组件设置合理的访问权限。

f) App自定义权限应严格按照操作系统权限要求定义和命名，确保完整、清晰、准确，并为权限配置合理的保护级别。

g) 以下操作应由用户主动触发，并在用户知情情况下执行:

1) 执行拨打电话、发送短信等操作;

2) 打开或关闭Wi-Fi、蓝牙、GPS等;

3) 拍摄、录音、截屏、录屏等;

4) 读写用户短信、联系人等个人信息。

h) 不应隐蔽收集个人信息，当录音、拍摄、录屏、定位等敏感功能在后台执行时，应采用显著方式（如图标闪烁、状态栏提示、自定义提示条等）提示用户。

i) 不应在用户不知情或未授权的情况下，通过隐蔽方式读取并上传剪切板中包含的个人信息和公共存储区中的个人信息。

j) 如操作系统支持，App申请相机、位置、麦克风等可收集个人敏感信息的权限宜提供用户选择临时单次授权。

k) 提供小程序接入平台的App，宜要求小程序向接入平台说明申请的系统权限及申请目的。

l) 提供小程序接入平台的App应为小程序提供权限管理的功能，小程序应允许用户关闭或撤回对小程序可收集个人信息权限的授权。

5 安卓系统典型权限的申请和使用要求

本章针对安卓 11 及以下版本给出了安卓系统典型权限的申请和使用要求，权限相关的业务功能示例参见附录 A 表 A.1。

5.1 日历权限（CALENDAR）

App应谨慎申请日历权限组中的权限，日历的访问应由用户主动触发。

5.2 通话记录权限（CALL_LOG）

除用户主动将App设置为默认电话应用，或为实现通话记录管理、备份恢复、骚扰电话拦截等功能，否则App不应向用户申请通话记录权限组中的权限。

5.3 相机权限（CAMERA）

App访问相机时，应在前台为用户呈现拍摄界面。

5.4 通讯录权限（CONTACTS）

a) 读写通讯录的行为应由用户主动触发，例如在添加通讯录好友的场景下，只有在用户实际使用到App的“添加通讯录好友”等功能时，才向用户申请权限并仅在此时读取通讯录。

注：除用户主动触发读写通讯录之外，还存在满足特定条件下自动读写通讯录的应用场景，如经用户授权根据通讯录变化向用户自动推荐 App 好友，此场景应经用户明示同意授权并严格在用户授权的使用范围内触发。

b) 应明确回传用户联系人数据的必要性，若实现相关功能不需要回传用户联系人数据，则不应回传。

5.5 位置权限（LOCATION）

a) 所提供业务功能与用户所在位置无关的App不应申请位置权

限。

b) 如操作系统支持，应允许用户在始终允许（前台和后台）、使用应用时允许（仅限前台）、单次允许（临时单次授权）、禁止获取位置信息四种位置状态中进行选择授权。

c) 除地图导航、运动健身等可能需要后台持续获取位置的服务类型外，其他服务类型不宜申请后台位置权限（ACCESS_BACKGROUND_LOCATION）。

d) 借助访问粗略位置权限（ACCESS_COARSE_LOCATION）即可实现相关业务功能的App，不建议申请精准位置权限（ACCESS_FINE_LOCATION）。

5.6 麦克风权限（MICROPHONE）

a) 麦克风的申请使用应由用户主动触发。

b) App持续使用麦克风时，应在前台以显式的方式提醒用户。

c) 用户完成使用后，App应立即停止访问麦克风。

5.7 电话权限（PHONE）

电话权限组所保护的数据和能力较多，App应结合业务功能需要仅申请必需的子权限。

a) 读取电话状态权限

1) 除安全风控场景外，App不应使用READ_PHONE_STATE权限读取不可变更的设备唯一标识符（如IMEI等），建议根据应用需要优先采用可变更的标识方案；

2) App监听设备的通话状态可通过接口PhoneStateListener或

请求AudioFocus实现，无需申请任何权限。

b) 拨打电话权限

1) 除非用户主动将App设置为默认电话应用或在紧急求救情况下，否则App不应向用户申请拨打电话权限；

2) 建议App采用其他不需要权限的替代方案来实现相关功能，例如使用Intent.ACTION_DIAL通过startActivity拉起系统拨号盘的方式进行拨号。

5.8 传感器权限（SENSORS）

除依托获取身体传感器信息权限（BODY_SENSORS）提供心率测量等功能的App外，其他App不应申请传感器权限。

5.9 短信权限（SMS）

a) 除非用户主动将App设置为默认短信应用，或实现短信管理、备份恢复、短信紧急求救等功能，否则App不应向用户申请短信权限。

b) 建议App采用其他替代方案来实现相关功能，例如使用Intent.ACTION_SENDTO通过startActivity拉起系统短信界面由用户点击后发送，这种发送短信的方式无需申请任何权限。

5.10 存储权限（STORAGE）

a) 如App不存在下载、读取外部存储文件的实际业务功能，可直接在App自有的目录下进行保存，不建议申请外部存储权限。

b) 建议优先使用MediaStore或SAF框架实现业务功能，而非申请外部存储权限直接进行读取。

5.11 其他要求

a) 安卓App的目标API等级应不低于23（targetSdkVersion>=23），目标API等级宜及时更新适配安卓新版本。

注：截至本实践指南发布时，推荐设置目标 API 等级不低于 28。

b) 除有特殊业务功能需求并征得用户明示同意外，安卓App不应申请使用设备管理器、辅助功能、监听通知栏、悬浮窗权限等特殊敏感权限。

注：特殊敏感权限，是指可访问移动智能终端特殊敏感功能的权限，一旦被恶意利用可能影响设备、系统、应用安全或侵犯用户隐私。安卓特殊敏感权限范围可参考附录 B。

c) 如安卓App确需申请使用设备管理器、辅助功能、监听通知栏、悬浮窗权限等特殊敏感权限，应向用户详细说明申请目的，并由用户到系统设置中手动打开。

附录 A 可收集个人信息权限

附录 A 给出了安卓和 iOS 可收集个人信息权限范围，其中表 A.1 的“业务功能示例”给出了与权限相关的业务功能示例，App 提供者在申请使用权限时可进行参考。

A.1 安卓可收集个人信息权限

安卓可收集个人信息权限，通常是安卓操作系统预定义保护级别（Protection Level）为危险（dangerous）级别的权限。此类权限与用户隐私和设备安全密切相关，需要 App 在运行时动态向用户申请。安卓 11 及以下版本的可收集个人信息权限详见表 A.1。

表 A.1 安卓可收集个人信息权限

序号	权限分组	权限名	功能描述	可访问的个人信息	业务功能示例
1	CALENDAR 日历	READ_CALENDAR 读取日历	允许 App 读取用户日历数据	系统日历中的日程安排、备忘、行程等信息	日程规划、事件提醒、票务预订等
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	用户通话记录	通话记录管理、备份与恢复，骚扰拦截、SOS 紧急求助等
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 监听呼出电话	允许 App 查看正在拨打的号码，并监听、控制或终止呼出电话	用户呼出的电话号码、呼叫状态等信息	呼出电话监控场景、儿童手表、骚扰拦截等

序号	权限分组	权限名	功能描述	可访问的个人信息	业务功能示例
6	CAMERA 相机	CAMERA 拍摄	允许 App 使用摄像头	照片或视频信息	拍摄照片视频、扫描二维码/条形码、人脸识别等
7	CONTACTS 通讯录	READ_CONTACTS 读取通讯录	允许 App 读取用户通讯录	联系人数据	通讯录管理与备份、添加联系人等
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	账户服务中的 App 账户列表	账号登录场景等
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	精准地理位置信息	定位当前用户位置、拍照记录照片拍摄位置、社交分享位置、O2O 上门服务定位用户位置等需要用户精准位置的场景
11		ACCESS_COARSE_LOCATION 访问粗略位置	允许 App 获取基于基站、IP 等粗略的地理位置	粗略地理位置信息	外卖、本地生活服务等分区域信息推荐、基于城市或地域进行新闻推送等基于粗略用户地理位置的场景

序号	权限分组	权限名	功能描述	可访问的个人信息	业务功能示例
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)	实时地理位置信息、行踪轨迹	地图导航、网络约车、运动健身等场景
13	MICROPHONE 麦克风	RECORD_AUDIO 录音	允许 App 使用麦克风进行录音	录音内容	语音即时通信、语音识别、音视频录制、直播等语音输入场景
14	PHONE 电话	READ_PHONE_STATE 读取电话状态	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	设备唯一标识信息(如 IMEI、设备序列号)	进行用户常用设备的标识,可用于监测 App 账户异常登录、关联用户行为
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	手机号码	读取本机号码场景,如运营商提供的快速一键登录功能

序号	权限分组	权限名	功能描述	可访问的个人信息	业务功能示例
16		CALL_PHONE 拨打电话	允许 App 直接拨打电话	实时通话行为	紧急电话或者提供电话管理功能
17		ANSWER_PHONE_CALLS 接听电话	允许 App 接听拨入的电话		在驾驶模式下直接接听来电等
18		ADD_VOICEMAIL 添加语音邮件	允许 App 向邮件中添加语音附件	语音邮件内容	
19		USE_SIP 使用网络电话	允许 App 拨打/接听 SIP 网络电话	实时网络通话行为	接听、拨打网络电话等
20		ACCEPT_HANDOVER 继续进行来自其他 App 的通话	允许 App 继续进行在其他 App 中发起的通话	实时网络通话行为	
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	心率等身体传感器数据	运动健身、健康类 App 及可穿戴设备显示心率等状况
22	SMS 短信	SEND_SMS 发送短信	允许 App 发送短信	短信	短信管理、短信备份恢复、手机号码注册或登陆时的验证码场景、SOS 紧急求助等
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	短信、彩信内容	

序号	权限分组	权限名	功能描述	可访问的个人信息	业务功能示例
25		RECEIVE_WAP_PUSH 接收 WAP 推送	允许 App 接收 WAP 推送信息	WAP 推送消息	短信管理、WAP 消息推送场景等
26		RECEIVE_MMS 接收彩信	允许 App 接收彩信	彩信	短信管理、接收彩信场景等
27	STORAGE 存储	READ_EXTERNAL_STORAGE 读取外置存储器	允许 App 读取外置存储器	外置存储器存储的个人数据	文件管理、阅读器等打开本地文件的场景等
28		WRITE_EXTERNAL_STORAGE 写入外置存储器	允许 App 写入外置存储器		存储拍摄的照片和视频，及下载文件、需要下载大量资源的游戏场景等
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	照片拍摄地点信息	展示照片拍摄地点的场景等
30	ACTIVITY_RECOGNITION 身体活动	ACTIVITY_RECOGNITION 识别身体活动	允许 App 识别身体活动	特定身体活动变化信息（如未移动、步行、跑步、骑车、坐车等）	追踪用户步数及卡路里消耗、需要对用户的身体活动进行分类的场景等

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；监听呼出电话（PROCESS_OUTGOING_CALLS）已在安卓 10 中废弃。

A.2 iOS可收集个人信息权限

iOS App通过在Information Property List文件（info.plist）中添加特定受保护资源的UsageDescription key，并将key的value设置为相应

受保护资源的使用目的说明的方式向操作系统申请权限。iOS 13及以下版本的可收集个人信息权限详见表A.2，iOS权限的使用场景可参考表A.1的“业务功能示例”。

表A.2 iOS可收集个人信息权限

序号	受保护的资源	权限名	功能描述	可访问的个人信息
1	Calendar and Reminders 日历与提醒事项	Calendars 日历	访问用户的日历数据	日历数据
2		Reminders 提醒事项	访问用户的提醒事项	提醒事项
3	Camera and Microphone 相机与麦克风	Camera 相机	访问设备的相机	拍摄的照片与视频
4		Microphone 麦克风	访问设备的麦克风	语音数据
5	Contacts 通讯录	Contacts 通讯录	访问用户的联系人	联系人数据
6	Face ID 面容 ID	FaceID 面容 ID	使用 Face ID 进行身份验证	面容 ID
7	Health 健康	Health Records 健康记录	读取临床健康记录	临床健康记录
8		Health Share 读取 HealthKit 健康数据	从 HealthKit 存储读取样本	健康数据
9		Health Update 更新 HealthKit 健康数据	将样本保存到 HealthKit 存储	健康数据
10	Home 家居	HomeKit 家居	请求访问用户的 HomeKit 配置数据	HomeKit 配置数据
11	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	位置信息
12		Location When In Use Usage 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	位置信息
13	MediaPlayer 媒体与 Apple Music	Media Library 媒体库	访问用户的媒体库	Apple Music、音乐和视频活动以及媒体资料库
14	Motion 运动与健身	Motion 运动与健身	访问设备的加速度计	身体活动、步数统计、已爬楼层数等在内的传感器数据

序号	受保护的资源	权限名	功能描述	可访问的个人信息
15	Photos 照片	Photo Library Additions 只写照片库	只写访问用户照片库	照片库
16		Photo Library 读取和写入照片库	读取和写入用户照片库	照片库
17	Speech 语音识别	Speech Recognition 语音识别	使用 Apple 的服务器执行语音识别（将用户数据发送至 Apple 的语音识别服务器）	语音数据

附录 B 安卓特殊敏感权限

由于某些特殊用途的App功能扩展的需要，安卓系统也提供了一些特殊的敏感权限。这些权限由于涉及到设备、系统、其他App的安全和用户体验，一旦被恶意App获取，可能侵犯用户隐私或设备安全，因此，通常只有少数App在少数场景才申请，建议提供单独管理界面详细说明申请目的，并适当增加障碍设计避免用户误操作。

表B.1 安卓特殊敏感权限

序号	权限名	功能描述	业务功能示例
1	BIND_DEVICE_ADMIN 设备管理器	允许App激活使用设备管理器	需对设备进行设置才允许在设备上办公的场景
2	BIND_ACCESSIBILITY_SERVICE 辅助模式	也称无障碍功能，允许App通过屏幕取词、模拟用户点击等方式，方便用户操作	无障碍人士使用场景
3	BIND_NOTIFICATION_LISTENER_SERVICE 监听通知栏	允许App监听其他App通知栏显示的内容	需要将通知栏内容引导到其它设备的场景
4	SYSTEM_ALERT_WINDOW 悬浮窗	允许App在其他App上覆盖显示	视频聊天、直播软件需要小窗体播放场景; 录屏软件、音乐软件等需要悬浮或桌面上显示的场景。
5	PACKAGE_USAGE_STATS 读取应用使用情况	允许App获取其他App的使用统计数据，例如使用频率、使用时长、语言设置等使用记录	应用商店、安全管理等需要监控应用的场景

附录 C 系统权限申请使用常见问题

附录B给出了App申请使用系统权限的常见问题，供App运营者申请使用系统权限时参考。

C.1 权限申请常见问题

a) 权限申请目的不明

1) 未告知申请目的

App 申请系统权限时未同步告知权限的申请目的，例如仅通过操作系统弹窗向用户申请系统权限，且未告知权限申请目的。

2) 目的告知不明确

例如将目的描述为“需要您开启存储权限，以保证存储相关功能的正常使用”，未具体明确地说明权限的使用目的。

b) 告知目的与实际不符

1) 实际申请权限超出或少于告知范围

未完整告知所申请的权限及其用于实现的功能或目的，或告知了实际并未申请的系统权限及其申请目的。

2) 告知内容存在错误或以虚假目的诱导用户同意

权限申请时告知内容与实际存在明显偏差、错误，或故意以并未真实提供的功能或实际并不存在的使用场景作为权限的申请目的，诱骗、误导用户同意授权。

c) 过度索权

1) 申请无关权限

部分所申请系统权限与 App 功能不相关，即不申请该等系统权限，App 也能够正常实现相应的功能。例如未提供短信相关功能的 App 申请短信权限。

2) 强制索取非必要权限

首先，App 存在强制索权情况（“不给权限就不能用”），即用户在打开 App 后或当使用到某项功能时，必须提供特定的系统权限，否则无法正常进入 App 或无法正常使用该功能；其次，App 所强制索取的系统权限并非其正常运行或实现相关功能所必需。例如浏览器 App 强制索要位置权限，用户拒绝提供位置权限则无法使用 App 任何功能。

3) 提前申请权限

App 在用户未触发相关功能或服务时，提前申请开启与其他功能相关但与当前功能无关的权限。例如 App 首次开启时便向用户申请 App 可能用到的所有系统权限，而其中部分系统权限所对应的功能尚未被用户主动触发，同时该等系统权限又与当前已触发的功能无关。

d) 强制捆绑授权

1) 必须同意开启App申请的所有权限，否则无法安装

在用户安装 App 时，以捆绑打包形式申请其向操作系统声明的所有权限，用户不同意则无法安装，安装完成后申请的所有权限默认打开（如安卓版 App 设置 targetSdkVersion 小于 23 所致）。

2) 频繁索权

对于用户可选提供的系统权限，在用户拒绝后，每当其重新打开 App 或进入相应界面，都会再次向用户索要或以弹窗等形式提示用户缺少相关权限，干扰用户正常使用。

C.2 权限使用常见问题

a) 权限滥用

违背已向用户告知并征得同意的权限使用目的、场景和规则等约定，恶意或以不正当方式使用获得的系统权限。例如利用悬浮窗权限设置全屏的透明弹窗，通过记录键盘操作窃取用户密码；利用读取电话状态及写入外置存储器权限，读取用户的设备唯一标识后将其写入外置存储器，供该用户安装的其他相关 App 读取用户的设备唯一标识等。

b) 隐蔽或超出预期收集使用个人信息

在用户不可感知或超出用户预期的情况下利用系统权限收集使用个人信息。例如在用户不可感知或超出用户预期的情况下读写、传输或使用用户的相册、语音备忘录、短信、联系人，通话记录、日历数据、传感器数据、位置信息、设备信息、已安装应用程序列表等；或在用户不可感知或超出用户预期的情况下使用设备的麦克风、相机等。

附录 D 常见服务类型不建议申请的安卓系统权限

基于技术检测和统计分析，附录 D 给出了地图导航等 30 种常见服务类型不建议申请的安卓系统权限，其中“×”表示该系统权限与对应服务类型的相关程度较低，除有特别明确合理的使用场景和申请理由外，否则不建议该服务类型申请。未标注为“×”的，不表示该权限为服务类型的必要权限，也不表示建议申请。App 运营者可识别 App 提供的服务类型，通过表 D.1-D.3 给出的服务类型与权限关系，综合判断 App 申请权限的合理性。

表 D.1 常见服务类型（1-10）不建议申请的安卓系统权限

序号	权限分组	权限名	地图导航	网络约车	即时通信	网络社区	网络支付	新闻资讯	网上购物	短视频	快递物流	餐饮外卖
1	CALENDAR 日历	READ_CALENDAR 读取日历	×	×	×						×	
2		WRITE_CALENDAR 编辑日历	×	×	×						×	
3	CALL_LOG 通话记录	READ_CALL_LOG 读取通话记录	×	×	×	×	×	×	×	×	×	×
4		WRITE_CALL_LOG 编辑通话记录	×	×	×	×	×	×	×	×	×	×
5		PROCESS_OUTGOING_CALLS 监听呼出电话	×	×	×	×	×	×	×	×	×	×
6	CAMERA 相机	CAMERA 拍摄										
7	CONTACTS 通讯录	READ_CONTACTS 读取通讯录	×									
8		WRITE_CONTACTS 编辑通讯录	×	×			×	×	×	×	×	×
9		GET_ACCOUNTS 获取 App 账户										
10	LOCATION 位置	ACCESS_FINE_LOCATION 访问精准定位										
11		ACCESS_COARSE_LOCATION 访问粗略位置										

序号	权限分组	权限名	地图导航	网络约车	即时通信	网络社区	网络支付	新闻资讯	网上购物	短视频	快递物流	餐饮外卖
12		ACCESS_BACKGROUND_LOCATION 支持后台访问位置			×	×	×	×	×	×	×	×
13	MICROPHONE 麦克风	RECORD_AUDIO 录音										
14	PHONE 电话	READ_PHONE_STATE 读取电话状态										
15		READ_PHONE_NUMBERS 读取本机电话号码	×	×			×	×		×		×
16		CALL_PHONE 拨打电话	×	×	×	×	×	×	×	×	×	×
17		ANSWER_PHONE_CALLS 接听电话	×	×	×	×	×	×	×	×	×	×
18		ADD_VOICEMAIL 添加语音邮件	×	×	×	×	×	×	×	×	×	×
19		USE_SIP 使用网络电话	×	×	×	×	×	×	×	×	×	×
20		ACCEPT_HANDOVER 继续进行来自其他 App 的通话	×	×	×	×	×	×	×	×	×	×
21	SENSORS 传感器	BODY_SENSORS 获取身体传感器信息	×	×	×	×	×	×	×	×	×	×
22	SMS 短信	SEND_SMS 发送短信	×	×	×	×	×	×	×	×	×	×
23		RECEIVE_SMS 接收短信	×	×	×	×	×	×	×	×	×	×
24		READ_SMS 读取短信	×	×	×	×	×	×	×	×	×	×
25		RECEIVE_WAP_PUSH 接收 WAP 推送	×	×	×	×	×	×	×	×	×	×
26		RECEIVE_MMS 接收彩信	×	×	×	×	×	×	×	×	×	×
27	STORAGE 存储	READ_EXTERNAL_STORAGE 读取外置存储器										
28		WRITE_EXTERNAL_STORAGE 写入外置存储器										
29		ACCESS_MEDIA_LOCATION 读取照片位置信息	×	×	×	×	×	×	×	×	×	×
30	ACTIVITY_RECOGNITION 身体活动	ACTIVITY_RECOGNITION 识别身体活动		×	×	×	×	×	×	×	×	×

表 D.2 常见服务类型（11-20）不建议申请的安卓系统权限

序号	权限分组	权限名	交通票务	婚恋相亲	求职招聘	网络借贷	房屋租售	二手车交易	运动健身	问诊挂号	网页浏览器	输入法
1	CALENDAR 日历	READ_CALENDAR 读取日历		×				×			×	×
2		WRITE_CALENDAR 编辑日历		×				×			×	×
3	CALL_LOG 通话记录	READ_CALL_LOG 读取通话记录	×	×	×	×	×	×	×	×	×	×
4		WRITE_CALL_LOG 编辑通话记录	×	×	×	×	×	×	×	×	×	×
5		PROCESS_OUTGOING_CALLS 监听呼出电话	×	×	×	×	×	×	×	×	×	×
6	CAMERA 相机	CAMERA 拍摄										
7	CONTACTS 通讯录	READ_CONTACTS 读取通讯录				×	×	×		×	×	
8		WRITE_CONTACTS 编辑通讯录		×	×	×	×	×	×	×	×	×
9		GET_ACCOUNTS 获取 App 账户										
10	LOCATION 位置	ACCESS_FINE_LOCATION 访问精准定位										×
11		ACCESS_COARSE_LOCATION 访问粗略位置										×
12		ACCESS_BACKGROUND_LOCATION 支持后台访问位置	×	×	×	×	×	×		×	×	×
13	MICROPHONE 麦克风	RECORD_AUDIO 录音										
14	PHONE 电话	READ_PHONE_STATE 读取电话状态										
15		READ_PHONE_NUMBERS 读取本机电话号码	×		×	×	×	×	×	×	×	×
16		CALL_PHONE 拨打电话	×	×	×	×	×	×	×	×	×	×
17		ANSWER_PHONE_CALLS 接听电话	×	×	×	×	×	×	×	×	×	×
18		ADD_VOICEMAIL 添加语音邮件	×	×	×	×	×	×	×	×	×	×
19		USE_SIP 使用网络电话	×	×	×	×	×	×	×	×	×	×

序号	权限分组	权限名	交通票务	婚恋相亲	求职招聘	网络借贷	房屋租售	二手车交易	运动健身	问诊挂号	网页浏览器	输入法
20		ACCEPT_HANDOVER 继续进行来自其他 App 的通话	×	×	×	×	×	×	×	×	×	×
21	SENSORS 传感器	BODY_SENSORS 获取身体传感器信息	×	×	×	×	×	×	×	×	×	×
22	SMS 短信	SEND_SMS 发送短信	×	×	×	×	×	×	×	×	×	×
23		RECEIVE_SMS 接收短信	×	×	×	×	×	×	×	×	×	×
24		READ_SMS 读取短信	×	×	×	×	×	×	×	×	×	×
25		RECEIVE_WAP_PUSH 接收 WAP 推送	×	×	×	×	×	×	×	×	×	×
26		RECEIVE_MMS 接收彩信	×	×	×	×	×	×	×	×	×	×
27	STORAGE 存储	READ_EXTERNAL_STORAGE 读取外置存储器										
28		WRITE_EXTERNAL_STORAGE 写入外置存储器										
29		ACCESS_MEDIA_LOCATION 读取照片位置信息	×	×	×	×	×	×	×	×	×	×
30	ACTIVITY_RECOGNITION 身体活动	ACTIVITY_RECOGNITION 识别身体活动	×	×	×	×	×	×			×	×

表 D.3 常见服务类型（21-30）不建议申请的安卓系统权限

序号	权限分组	权限名	安全管理	旅游服务	酒店服务	网络游戏	在线影音	儿童教育	电子图书	拍摄美化	应用商店	网络直播
1	CALENDAR 日历	READ_CALENDAR 读取日历	×		×					×		
2		WRITE_CALENDAR 编辑日历	×							×		
3	CALL_LOG 通话记录	READ_CALL_LOG 读取通话记录		×	×	×	×	×	×	×	×	×
4		WRITE_CALL_LOG 编辑通话记录		×	×	×	×	×	×	×	×	×
5		PROCESS_OUTGOING_CALLS 监听呼出电话		×	×	×	×	×	×	×	×	×
6	CAMERA 相机	CAMERA 拍摄										
7	CONTACTS 通讯录	READ_CONTACTS 读取通讯录						×	×	×	×	×
8		WRITE_CONTACTS 编辑通讯录		×	×	×	×	×	×	×	×	×
9		GET_ACCOUNTS 获取 App 账户										
10	LOCATION 位置	ACCESS_FINE_LOCATION 访问精准定位	×					×	×		×	
11		ACCESS_COARSE_LOCATION 访问粗略位置	×						×			
12		ACCESS_BACKGROUND_LOCATION 支持后台访问位置	×	×	×	×	×	×	×	×	×	×
13	MICROPHONE 麦克风	RECORD_AUDIO 录音										
14	PHONE 电话	READ_PHONE_STATE 读取电话状态										
15		READ_PHONE_NUMBERS 读取本机电话号码						×	×	×	×	
16		CALL_PHONE 拨打电话		×	×	×	×	×	×	×	×	×
17		ANSWER_PHONE_CALLS 接听电话		×	×	×	×	×	×	×	×	×
18		ADD_VOICEMAIL 添加语音邮件	×	×	×	×	×	×	×	×	×	×
19		USE_SIP 使用网络电话	×	×	×	×	×	×	×	×	×	×
20		ACCEPT_HANDOVER 继续进行来自其他 App 的通话	×	×	×	×	×	×	×	×	×	×

序号	权限分组	权限名	安全管理	旅游服务	酒店服务	网络游戏	在线影音	儿童教育	电子图书	拍摄美化	应用商店	网络直播
21	SENSORS 传感器	BODY_SENSORS 获取身体传感器信息	×	×	×	×	×	×	×	×	×	×
22	SMS 短信	SEND_SMS 发送短信		×	×		×	×	×	×	×	×
23		RECEIVE_SMS 接收短信		×	×	×	×	×	×	×	×	×
24		READ_SMS 读取短信		×	×		×	×	×	×	×	×
25		RECEIVE_WAP_PUSH 接收 WAP 推送		×	×	×	×	×	×	×	×	×
26		RECEIVE_MMS 接收彩信		×	×	×	×	×	×	×	×	×
27	STORAGE 存储	READ_EXTERNAL_STORAGE 读取外置存储器										
28		WRITE_EXTERNAL_STORAGE 写入外置存储器										
29		ACCESS_MEDIA_LOCATION 读取照片位置信息	×	×	×	×	×	×	×	×	×	×
30	ACTIVITY_RECOGNITION 身体活动	ACTIVITY_RECOGNITION 识别身体活动	×	×	×	×	×	×	×	×	×	×

注：附录 D 主要是针对大众用户使用的 App 给出的建议，不包括服务提供者所使用的 App（如网约车司机 App，外卖、快递配送员 App 等），此外，也不包括智能手表等可穿戴设备。