ICS 33.050
M 30

团　体　标　准

T/TAF 067-2020

移动智能终端与应用软件用户个人信息保护实施指南 第6部分：应用软件权限规范

Mobile intelligent terminal and application software user personal information protection implementation guide—Part 6: Application software sensitive access specification

2020-08-24 发布　　2020-08-24 实施

电信终端产业协会　发布

目　次

前　言

本标准是移动智能终端及应用软件用户个人信息保护实施指南系列标准的第六部分，主要针对应用软件的敏感权限申请和使用进行规范和要求。本标准首先对用户敏感信息的信源进行了定义，并在此基础上，说明了与信源对应及关联的敏感权限，进而声明了应用软件申请和使用敏感权限时应遵循的原则，最后以附录举例的方式，不完全地枚举了应用软件在具体功能和场景下，可合理使用的敏感权限。

标准按照 GB/T 1.1-2009 给出的规则起草。

本标准中的某些内容可能涉及专利。本标准的发布机构不承担识别这些专利的责任。

本标准由电信终端产业协会提出并归口。

本标准起草单位：中国信息通信研究院、武汉安天信息技术有限责任公司、北京百度网讯科技有限公司、华为技术有限公司、维沃移动通信有限公司、OPPO广东移动通信有限公司、北京奇虎科技有限公司、北京小米科技有限责任公司、宏达通讯有限公司。

本标准主要起草人：宁华、王艳红、王宇晓、董雾、罗成、刘波、黄莹、张屹、姚一楠、李笑如、王江胜、贾科、焦四辈、李腾、周圣炎、张朝、王安宇、衣强、赵新娜、樊俊燕。

引　言

移动智能终端应用软件为终端用户提供种类繁多、功能各异的服务，由于应用开发者、终端用户对移动智能终端应用软件的权限获取合理性关注较少，目前没有形成明确的监管及合理的权限安全管理机制，移动智能终端应用软件要求终端用户授予安卓权限时，可能存在没有根据自身应用功能需求来合理申请或调用权限的行为，从而造成权限被滥用，存在较大安全威胁，进而导致用户个人信息存在泄露风险。

综上所述，为了提供给移动终端用户更加完善的服务，提高整个行业市场更广的发展前景，维护国内安全可信的信息通信网络环境，移动智能终端应用软件敏感权限规范的颁布是非常有必要的。该标准将适用于智能终端生产企业的移动智能终端预置应用软件，和互联网信息服务提供者提供的移动智能终端应用软件，积极响应我国移动互联网市场安全环境的大方向，贴合移动智能终端及应用行业健康持续发展道路。

移动智能终端与应用软件用户个人信息保护实施指南 第6部分：应用软件权限规范

1 范围

本标准规定了移动应用软件敏感权限规范要求和实施指南。

本标准适用于移动智能终端预置应用软件以及互联网信息服务提供者提供的可以通过移动智能终端下载、安装、升级的应用软件。

2 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

YD/T 2407-2013 《移动智能终端安全能力技术要求》；

YD/T 2439-2012 《移动互联网恶意程序描述格式》；

YD/T 3228-2017 《移动应用软件安全评估方法》；

《关于加强移动智能终端进网管理的通知》（工信部电管〔2013〕120号）；

《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管[2016]407号）。

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

移动智能终端 smart mobile terminal

移动智能终端是指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终端产品。

3.1.2

移动应用软件 mobile application software

移动智能终端应用软件（以下简称“应用软件”）是指移动智能终端预置以及通过网站、应用商店、扫二维码、应用自身、其他线上线下平台或渠道下载、安装、升级、卸载的应用软件。

3.1.3

个人信息 personal information

与一个身份已被识别或者身份可被识别的自然人（“数据主体”）相关的任何信息；身份可识别的自然人是指其身份可以通过诸如姓名、身份证号、位置数据等识别码或者通过一个或多个与自然人的身体、生理、精神、经济、文化或者社会身份相关的特定因素来直接或者间接地被识别。个人数据包括：

自然人的email地址、电话号码、生物特征（指纹）、位置数据、IP地址、医疗信息、宗教信仰、社保号、婚姻状态等。

3.1.4

敏感权限 sensitive permission

敏感权限对应的数据或资源，涉及下列范围：个人信息或个人敏感信息，一旦泄露、非法提供或滥用可能危害人身和财产安全；对用户存储的数据或其他应用的操作产生影响，可能干扰系统正常运行或实施恶意行为。

4 应用软件敏感权限规范安全准则

4.1 概述

移动智能终端应用可以通过申请并获取相应的权限，从而得以对终端用户的个人信息执行创建、获取、存储、传输、修改、删除等操作，即相关权限是用户个人信息得以产生的前提和必要条件。因此，如要针对移动智能终端及应用软件用户的个人信息实施保护，移动应用对相应权限的申请及使用就必须要进行有效地规范和管理，防止和管控移动应用因申请多余的、无关的权限以及滥用权限而导致用户个人信息泄露的问题。

用户个人信息的信源，即在移动智能终端上产生各类用户个人信息的实体和来源。移动智能终端操作系统通过权限管理，对信源产生的各类用户信息的访问和使用进行管控，相应地，终端应用在访问和使用信源产生的用户数据之前，需要合规地声明、申请和使用对应的权限。

不同的用户个人数据由不同的信源产生，也对应不同的系统权限，下面对信源的类别和范围进行说明。

4.2 用户个人信息的信源范围定义

4.2.1 定位

通过使用定位权限，可实现提供地理位置信息。

4.2.2 摄像头

通过使用摄像头权限，可实现执行拍照、录像等功能以获取图片、视频等信息。

4.2.3 麦克风

通过使用麦克风权限，可实现录音以获取音频信息。

4.2.4 电话

通过使用电话权限，可实现拨打电话、读写通话记录、获取终端识别码等信息。

4.2.5 信息

通过使用信息权限，可实现创建、发送、接收、读取和修改等操作的短信、彩信等信息。

4.2.6 联系人

通过使用联系人权限，可实现读取、创建、修改、删除联系人等信息。

4.2.7 存储空间

通过使用应用存储空间的权限，可实现在存储空间中执行搜索、创建、读取、修改文件等信息。

4.2.8 日程表

通过使用日程表权限，可实现创建、读取、修改和删除日历等信息。

4.2.9 传感器

通过使用传感器权限，可实现获取使用者身体特征信息，包括心率、体温、步频、睡眠数据等信息。

4.3 应用软件敏感权限规范基本要求

a）应用软件申请敏感权限时必须有明确、合理的业务功能和使用场景，不应申请与应用业务功能无关的其他权限。

b）应用软件申请敏感权限时或申请之前，应明确逐条告知用户，申请和使用某权限的目的、方式和范围。

c）应用软件不以默认、捆绑、停止安装使用等手段变相强迫用户授予敏感权限申请。

d）应用软件申请敏感权限时，应允许用户拒绝授权，并且不能因用户拒绝授权提供服务最小必要的权限之外的敏感权限而自动关闭、退出软件或禁止其他无关功能的使用，也不应频繁申请，干扰用户使用应用软件其他功能。

e）应用软件在用户授权后，应允许用户撤回授权，并且不能因用户撤回某项授权而禁止用户使用与该敏感权限无关的功能和业务，或者完全禁止用户使用应用软件。

f）应用软件对敏感权限的使用应符合权限申请时声明的目的、方式和范围，并不得在未获得用户授权的前提下，将权限对应的数据或能力对外提供。

4.4 应用软件权限具体要求

4.4.1 位置权限

位置权限包括访问精确位置、访问粗略位置、后台访问位置，允许应用软件在应用使用时获得位置信息、始终可获得位置信息、或禁止获得用户位置信息。

除出行、导航、运动健康类应用可申请后台访问位置信息，禁止其它类应用申请后台访问用户位置信息。

定位服务仅需申请粗略位置权限、且单次获取用户当前位置，无需高精度持续跟踪用户，减少对设备功耗的影响。

4.4.2 相机权限

应用访问相机时，必须在前台为用户呈现显示的拍摄界面。

4.4.3 麦克风权限

麦克风权限的使用必须是由用户主动触发，用户使用完后，应用必须立即停止继续访问麦克风。应用持续使用麦克风权限时，系统在前台以显性的方式提醒用户。

4.4.4 电话权限

只有在用户主动将应用注册为默认电话程序的情况下，应用才可以向用户申请拨打电话权限。

应用监听设备的通话状态可以通过系统提供的接口实现，无需申请任何权限即可使用。

系统已经禁止了通过申请“读取手机识别码”权限，应用软件应使用其它ID，如OAID作为替代方案。

4.4.5 短信息权限

短信属于高度敏感的个人数据，应用禁止申请此权限组，只有在用户主动将应用注册为默认短信的情况下，应用可向用户申请发送短信权限。建议应用采用系统提供的接口来实现应用功能，无需申请任何权限，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。

4.4.6 通讯录权限

通过通讯录属于敏感的个人数据，与用户无关的功能禁止访问通讯录。即使是用户所需功能，也需在用户主动触发时应用才读写通讯录。如应用需要用户的通讯录在应用用户中查找朋友，只有在用户使用应用的“添加朋友”功能时，应用才申请权限并仅在此时去读取通讯录。

应用应谨慎使用删除通讯录权限。

4.4.7 存储空间权限

应用不需要对外分享、下载、读取外部存储上的文件情况下，不应申请存储权限，可直接保存在应用自有的目录下。

4.4.8 日历权限

日历的访问也必须由用户主动触发，禁止应用在用户不可感知或超出预期的情况下访问日历。日历属于敏感的个人数据，与用户无关的功能禁止访问日历。

4.4.9 传感器权限

传感器权限涉及到用户敏感数据，只有运动健康类应用软件可以申请个人敏感信息相关的传感器权限。

4.5 信源与软件应用场景化分类

移动智能终端应用软件为保证功能和业务的正常运行，在运行和服务提供过程中可能需要申请和授予单一或多元信源的访问和使用权限。即针对某个具体的应用软件使用场景和功能，应用软件申请哪些对应的敏感权限是必需的或合理的，对这些映射关系进行说明和界定。敏感权限及其对应的常用功能场景，请参考附录A。

4.6 基于差异化和融合场景的应用权限规范

移动互联网仍然不断演进，移动应用的新功能和新的业务场景也不断涌现。同时，综合了多项功能和使用场景的融合移动应用也逐渐增多。本标准的第二部分（第4章节），即针对单个权限及其对应的使用场景说明和规范，针对上述情景并不能做到全覆盖。

因此，针对未在第4章节列出和说明的移动应用新增功能和业务场景，其权限的申请和使用，都必须遵循4.3章“应用软件权限敏感规范基本要求”的各项规定和要求。

附 录 A
（资料性附录）
敏感权限对应的常用功能场景列表

表A.1 位置信息场景

功能场景类型	场景说明和举例
出行服务	定位用户和司机信息，明确用车起点和目的地，便于计费。
导航服务	精准定位起始地和目的地，根据起始地和目的地精准计算路线。
O2O 上门服务	精准定位用户位置信息，进行基于位置信息的上门服务。
社交通讯	以用户的位置为中心，定位周边好友，或根据用户与好友之间的位置，计算距离，进行路线规划。
电商购物	根据用户的精准定位，分区域的进行商品、店铺或服务等推荐；根据用户定位信息，自动填写收货地址。
影音娱乐	基于用户的地理位置，推荐周边的有趣视频；根据用户所看的视频，推荐周边与用户看同一视频的其他用户，增强社交属性。
新闻阅读	利用精准定位，获取用户所在城市、区域，推荐给用户本地的新闻内容。
天气服务	向用户提供具体位置和地点的天气信息。
快递配送	通过对快递服务定位，使得收发双方可以实时看到物品地点。

表A.2 照相机场景

功能场景类型	场景说明和举例
拍照和视频录制	用户为记录、上传、分享、扫码等原因，主动拍摄照片和视频；
手电筒	开启手电筒需要申请照相机权限；
身份验证	注册、登录时需要开启相机，协助身份认证；
条码扫描	通过条码、二维码扫描进行相关操作。

表A.3 麦克风场景

功能场景类型	场景说明和举例
社交通信	例如聊天应用，用于录制语音信息；

文本输入	例如输入法，用于语音输入；
语音控制	例如使用语音控制 IoT 设备的移动应用，用于录制语音指令；
移动办公	例如使用录音机等进行信息记录、识别等操作；
多媒体处理	例如短视频类应用，录制音频、视频等需求；
语言学习	例如外语学习，发音训练等；

表A.4 电话场景

功能场景类型	**场景说明和举例**
社交通信	例如拨打互联网电话；
数据备份	例如备份工具需要访问通话记录进行数据备份；
通话记录管理	例如骚扰拦截等；

表A.5 信息场景

功能场景类型	**场景说明和举例**
信息管理	用于收发和管理短彩信状态的应用软件，可申请信息读、写、接收和发送权限；
数据备份	例如备份工具需要访问通话记录进行数据备份；

表A.6 联系人场景

功能场景类型	**场景说明和举例**
通信录管理	用于新建、保存、修改和删除等联系人管理应用软件，可申请联系人读和写权限，例如名片、电话本管理等工具软件；
数据备份	通过备份工具软件备份联系人，可以申请联系人读权限；
网络电话	网络拨打电话应用软件，可申请联系人读权限；
移动办公	例如办公软件、邮件工具软件等，可申请联系人读和写权限；

表A.7 存储场景

功能场景类型	**场景说明和举例**
新建和保存	用户在使用应用过程中需要在本应用的缓存目录外创建或保存文件，可申请存储空间

	写权限。例如办公工具新建和保存文件，相机、录音、视频应用生成的媒体文件，浏览器等在线阅读工具下载的网络文件，游戏下载的资源文件等；
文件分享	用户在使用应用过程中需要访问、分享移动智能终端文件，可申请存储空间读权限，例如社交软件分享办公文件、媒体文件等；
文件编辑	用户在使用应用过程中需要修改移动智能终端的文件，可申请存储空间读和写权限，例如办公软件，图片、视频等媒体编辑软件等；
文件清理	用户在使用应用过程中需要删除移动智能终端的文件，可申请存储空间读和写权限，例如空间清理工具软件等；
阅读工具	用户在使用应用过程中需要打开移动智能终端的文件，可申请存储空间读权限，例如阅读器等软件等；

表A.8 日程表场景

功能场景类型	**场景说明和举例**
时间管理	例如 GTD 类工具；
日历应用	例如万年历类工具；
学习办公	例如制定学习和工作计划，邮件管理工具等；
生活服务	票务预订、提醒，旅游类应用等；
信息记录	例如生日，重大事件提醒等；

表A.9 传感器场景

功能场景类型	**场景说明和举例**
运动健康	例如用于记录用户心率等运动数据的应用等；
可穿戴应用	例如将手机与可穿戴设备等终端设备相互连接和数据通信的应用等；

电信终端产业协会团体标准

移动智能终端与应用软件用户个人信息保护实施指南 第 6 部分：应用软件权限规范

T/TAF 067-2020

*

电信终端产业协会印发

地址：北京市西城区新街口外大街 28 号

电话：010-82052809

电子版发行网址：www.taf.org.cn