

ICS 33.050

M 30

团 体 标 准

T/TAF 081.1-2021

移动智能终端应用软件调用行为记录能力 要求 总则

Applications call behavior record capability requirements of
smart phone—

General principle

2021-01-08 发布

2021-01-08 实施

电信终端产业协会 发布

目 次

前言	II
引言	III
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
3.1 术语和定义	1
3.2 缩略语	2
4 移动智能终端应用软件调用行为类型分类	2
4.1 分类概述	2
4.2 按总额统计	2
4.3 按次统计	2
5 移动智能终端应用软件调用行为记录内容要求	2
5.1 按总额统计类型调用行为记录内容要求	2
5.2 按次统计类型调用行为记录内容要求	3
6 移动智能终端应用软件调用行为记录技术能力要求	4
6.1 概述	4
6.2 调用行为记录作用范围	4
6.3 调用行为记录准确性要求	4
6.4 调用行为记录防篡改要求	4
7 移动智能终端应用软件调用行为的记录、保存、展示和删除要求	4
7.1 记录要求	4
7.2 保存要求	4
7.3 展示要求	4
7.4 删除要求	5
8 移动智能终端应用软件调用行为记录的安全等级要求	5
附录 A（资料性）调用行为记录展示示例	7

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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、OPPO广东移动通信有限公司、博鼎实华（北京）技术有限公司、华为技术有限公司、维沃移动通信有限公司、高通无线通信技术（中国）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、微软（中国）有限公司、华硕电脑（上海）有限公司。

本文件主要起草人：邹海荣、李腾、宁华、董雾、王江胜、衣强、贾科、詹维骁、吴春雨、姚一楠、赵中杰、刘献伦、梅小虎、游苏英、林志泳、斯加权、陶永。



引 言

移动智能终端设备应用程序的爆发式发展，使得应用程序的功能越发强大，同时为了实现丰富的功能服务，应用程序需要操作系统授予的权限也种类繁多，其中不乏与用户隐私密切相关的权限。操作系统在授予应用程序权限后，缺乏有效的管控、监督机制，导致部分应用程序在获取权限后可以在用户无感知的情况下调用获取用户隐私数据的功能，即使发生隐私泄露事件，也无有效的记录查证。

应用程序的调用行为由于缺乏有效的记录，部分恶意应用的隐私窃取行为愈发猖獗。所以，出于对用户个人信息保护的需要，应用程序调用行为记录能力要求迫切需要出台。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。本文件将适用于可安装由第三方开发者开发的应用程序的移动智能终端，为移动智能终端厂商设计应用程序调用行为记录提供依据。



移动智能终端应用软件调用行为记录能力要求 总则

1 范围

本文件规定了应用软件调用行为记录能力的要求，包括：调用行为类型分类、调用行为内容记录要求、调用行为记录技术能力要求、调用行为的记录、保存、展示和删除要求。

本文件适用于各种制式的移动智能终端，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 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2010 信息安全技术 术语

YD/T 2407 移动智能终端安全能力技术要求

3 术语、定义和缩略语

3.1 术语和定义

YD/T 2407界定的以及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

能够接入移动通信网，具有能够提供应用软件开发接口的操作系统，具有安装、加载和运行应用软件能力的终端。

3.1.2

用户 user

使用移动智能终端资源的对象，包括人或第三方应用软件。

3.1.3

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

运行在移动智能终端上的系统软件，控制、管理移动智能终端上的硬件和软件，提供用户操作界面、应用软件编程接口和其他系统服务的应用软件。

3.1.4

移动智能终端应用软件 smart mobile terminal application

移动智能终端内，能够利用移动智能终端操作系统提供的开发接口，实现某项或某几项特定任务的计算机软件或者代码片段。包含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网站、应用商店等移动应用分发平台下载、安装、升级的应用软件。

3.1.5

移动智能终端预置应用软件 smart mobile terminal preloaded application

移动智能终端内，在主屏幕和辅助屏界面（不包含进入界面后，通过菜单进入或者调起的功能）有用户交互入口并且可独立使用的移动智能终端应用软件。

3.2 缩略语

下列缩略语适用于本文件。

APP 应用软件 Application

4 移动智能终端应用软件调用行为类型分类

4.1 分类概述

移动智能终端应用软件调用行为根据行为产生的结果类型不同，可分为：按总额统计、按次统计。移动智能终端操作系统根据调用行为类型的差异使用不同的记录方式。

4.2 按总额统计

按总额统计指应用软件的调用行为在一定时间周期内所产生的累计数据。例如，应用软件调用移动通信网络产生的流量数据属于按总额统计。

4.3 按次统计

按次统计指应用软件的调用行为在单位时间周期内所产生的单次数据。例如，应用软件最近一次调用位置信息属于按次统计记录。

5 移动智能终端应用软件调用行为记录内容要求

5.1 按总额统计类型调用行为记录内容要求

按总额统计类型记录的内容至少应包含：应用软件名称、调用行为名称、总额数据。总额数据可持续累计或周期性累计（如每7天、每自然月等）。按总额统计调用行为记录精度要求如下表1：

表 1 按总额统计调用行为记录精度要求

调用行为名称	记录精度
调用移动通信网络	1Byte上/下行流量

注：表格中未列举的调用行为可自行设计记录精度。

5.2 按次统计类型调用行为记录内容要求

按次统计类型记录的内容至少应包含：应用软件名称、调用行为名称、调用行为起始时间，时间精度至少为分钟。可增加调用结果记录：已允许/已禁止、调用时应用软件所处前后台等信息。按次统计类型的调用行为记录精度要求如下表2所示：

表 2 按次统计调用行为记录精度要求

调用行为名称	记录精度
获取定位	每次调用
进行通话录音	每次调用
本地录音	每次调用
后台截屏/录屏	每次调用
拍照/摄像	每次调用
读取媒体影音数据（如照片、视频和音频）	每次调用
读取生物特征数据（如指纹识别、人脸识别等）	每次调用
读取设备唯一可识别信息	每次调用
发送短信	每次调用
拨打电话	每次调用
发起三方通话	每次调用
接收短信	每次调用
发送彩信	每次调用
读取电话本	每次调用
读取通话记录	每次调用
写删短信	每次调用
写删彩信	每次调用
写删电话本	每次调用
写删通话记录	每次调用
写删日程表	每次调用
读取日程表	每次调用
读取上网记录	每次调用
读取短信	每次调用
读取彩信	每次调用

注1：上网记录数据包括浏览记录及书签。

注2：日程表及上网记录数据的操作要求仅针对有标准API或有其他通用调用方式的情况，第三方应用软件的私有数据如无法访问则不做要求。

注3：本文件生物特征识别信息（如指纹识别、人脸识别等）指对处于任何处理阶段的生物特征样本、生物特征参考、生物特征项或生物特征的通称。

注4：本文件设备唯一标识信息主要指不可重置的设备标识符，如IMEI、MAC（WLAN的不可修改的物理地址）。

注5：读取媒体影音数据（如照片、视频和音频）仅记录通过通用接口（媒体库方式）访问的行为，文件系统方式访问的行为不做强制要求。

注6：表格中未列举的调用行为可自行设计记录精度。

6 移动智能终端应用软件调用行为记录技术能力要求

6.1 概述

移动智能终端应用软件的调用行为记录作为其在移动智能终端表现的完整反馈,对操作系统技术能力提出了一定要求,以保证调用行为记录的完整性、真实性、有效性。

6.2 调用行为记录作用范围

移动智能终端操作系统对应用软件的调用行为记录应包含非自研预置应用软件和第三方应用软件,确保上述应用的调用行为能完整记录,不出现遗漏。

6.3 调用行为记录准确性要求

移动智能终端操作系统对调用行为的记录应在第三方应用已获得相应调用行为的权限授权后开始记录,调用行为的起始时间为第三方应用调用相应功能接口或鉴权接口的时间。

移动智能终端操作系统对调用行为的记录应在行为发生起始时间1分钟内生成,确保记录内容(4.1、4.2)的准确性,不应出现记录内容缺失、错误现象。

6.4 调用行为记录防篡改要求

移动智能终端操作系统应提供调用行为记录数据保护机制,防止调用行为记录数据库被恶意删除、篡改,用户及第三方应用软件不能访问调用行为记录的原始数据库文件。

7 移动智能终端应用软件调用行为的记录、保存、展示和删除要求

7.1 记录要求

移动智能终端操作系统应至少提供《移动智能终端安全能力技术要求》5.5.2.中的a)类调用行为的记录能力。厂商可根据终端配置水平的差异提供可配置调用行为是否记录的功能,如提供该项功能,用户可自主选择是否对调用行为记录进行单项配置,用户的修改可覆盖厂商的默认配置。

7.2 保存要求

操作系统对不同类型的调用行为提供不同的保存期限,按总额统计的调用行为保存期限至少应支持到当前自然月天数,按次统计的调用行为保存期限应满足系统最低要求,保存期限可适当延长,但不应缩短。

7.3 展示要求

操作系统应提供调用行为记录展示的能力供用户查看。如操作系统不支持的调用行为,可不做记录和展示。展示形式可包括但不限于列表、图表等形式。

按总额统计类型调用行为的展示:展示内容至少可查看周期内累计总额,展示形式包含应用软件名称、调用行为名称、数据总额。数据总额可持续累计或周期性累计(如每自然月等)。展示方式可参考附录A中的流量数据统计展示。

按次统计类型调用行为的展示：展示内容至少为保存期限内最后一次详情或每次详情，展示形式包含应用软件名称、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），可增加调用结果记录：已允许/已禁止、调用时应用软件所处前后台等信息。展示方式可参考附录A中的按次统计调用行为展示。

7.4 删除要求

操作系统应提供调用行为记录到期或所有记录总数超过一定数量自动删除的能力，调用行为记录到达最大保存期限或所有记录总数超过一定数量后，自动删除超出阈值部分，删除操作遵循由旧到新的删除原则，优先删除最早的记录，阈值可根据终端配置水平的差异做调整。操作系统也可提供手动删除调用行为记录的能力。记录总数达到阈值而保存期限未到期时，自动删除视为符合要求。

8 移动智能终端应用软件调用行为记录的安全等级要求

移动智能终端应用软件调用行为记录的安全等级要求对应移动智能终端安全能力分级要求。其中必选的调用行为记录对应移动智能终端安全能力为一级的要求（《移动智能终端安全能力技术要求》5.5.2中的a)类调用行为）；其他可选要求根据移动智能终端安全能力等级要求选择（安全能力五级要求（《移动智能终端安全能力技术要求》5.5.2中的b)类调用行为）在必选调用行为的基础上不得少于3项可选的调用行为记录。具体调用行为的要求如下表3所示：

表3 调用行为记录等级要求

调用行为名称	记录必选要求
调用移动通信网络	必选
获取定位	必选
进行通话录音	必选
本地录音	必选
后台截屏/录屏	必选
拍照/摄像	必选
读取媒体影音数据（如照片、视频和音频）	必选
读取生物特征数据（如指纹识别、人脸识别等）	必选
读取设备唯一可识别信息	必选
发送短信	可选
拨打电话	可选
发起三方通话	可选
接收短信	可选
发送彩信	可选
读取电话本	必选
读取通话记录	可选
写删电话本	可选
写删短信	可选
写删彩信	可选
写删通话记录	可选

表3 调用行为记录等级要求（续）

写删日程表	可选
读取日程表	可选
读取上网记录	可选
读取短信	必选
读取彩信	可选

注：如操作系统不再支持三方应用读取设备唯一可识别信息，可不设为必选。



附录 A (资料性) 调用行为记录展示示例

A.1 按次统计调用行为记录

图 A.1 是按次统计调用行为记录的示例：默认展示最近 X 天所有的调用行为记录详情，支持以“权限”、“应用”维度管理查看。



图A.1按次统计调用行为记录示例

A.2 调用行为记录配置

图A.2是调用行为记录配置示例：可配置需要记录的调用行为，关闭对应行为开关则对所有应用软件停止该项调用行为记录。



图A.2 调用行为记录配置示例

A.3 流量数据统计展示

图A.3是流量数据统计展示的示例：记录当前自然月应用调用的流量数据总额。



电信终端产业协会团体标准

移动智能终端应用软件调用行为记录能力要求 总则

T/TAF 081.1-2021

*

版权所有 侵权必究

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