

ICS 33.050
CCS M 30

团体标准

T/TAF 077.11—2022
代替 T/TAF 077.11—2021

APP 收集使用个人信息最小必要评估规范 第 11 部分：通话记录

Application software user personal information collection and usage
minimization and necessity evaluation specification—

Part 11: Call log

2022-09-15 发布

2022-09-15 实施

电信终端产业协会 发布

目 次

前言	II
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	1
5 基本原则	2
6 通话记录信息分类	2
7 处理通话记录典型应用场景	2
8 评估要求	2
8.1 告知同意	2
8.2 权限要求	3
8.3 收集阶段	3
8.4 存储阶段	4
8.5 使用阶段	4
8.6 提供阶段	4
8.7 删除阶段	5
9 评估方法	5
9.1 告知同意	5
9.2 权限要求	5
9.3 收集阶段	6
9.4 存储阶段	6
9.5 使用阶段	7
9.6 提供阶段	7
9.7 删除阶段	8

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。

本文件是T/TAF 077《APP收集使用个人信息最小必要评估规范》的第11部分。T/TAF 077已经发布了以下部分：

- 第1部分：总则；
- 第2部分：位置信息；
- 第4部分：通讯录；
- 第5部分：设备信息；
- 第6部分：软件列表；
- 第7部分：人脸信息；
- 第8部分：录像信息；
- 第9部分：短信信息；
- 第10部分：录音信息；
- 第11部分：通话记录；
- 第12部分：好友列表；
- 第13部分：传感器信息；
- 第14部分：应用日志信息；
- 第15部分：房产信息；
- 第16部分：交易记录；
- 第17部分：身份信息；
- 第18部分：剪切板信息。

本文件代替 T/TAF 077.11—2021《APP收集使用个人信息最小必要评估规范 通话记录》，与 T/TAF 077.11—2021 相比，除结构调整和编辑性改动外，主要的技术变化如下：

- a) 增加了“通话记录信息分类”一章（见第6章）；
- b) 更改了标题，细分了应用场景类型（见第7章，2021年版的第5章）；
- c) 增加了“评估要求”一章（见第8章）；
- d) 增加了“告知同意”、“权限要求”描述（见8.1、8.2）；
- e) 更改了“收集阶段”要求（见8.3，2021年版的7.1）；
- f) 更改了“存储阶段”要求（见8.4，2021年版的7.3）；
- g) 更改了“使用阶段”要求（见8.5，2021年版的7.2）；
- h) 增加了“提供阶段”要求（见8.6）；
- i) 更改了“删除阶段”要求（见8.7，2021年版的7.4）；
- j) 更改了“评估方法”要求（见第9章，2021年版的第8章）。

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、北京奇虎科技有限公司、泰尔认证中心有限公司、华为技术有限公司、北京字节跳动科技有限公司、维沃移动通信有限公司、OPPO广东移动通信有限公司、荣耀终端有限公司、北京快手科技有限公司、博鼎实华（北京）技术有限公司。

本文件主要起草人：姚一楠、宁娇、任海峰、吴怡、衣强、王宇晓、贾科、李腾、宁华、王艳红、赵晓娜、落红卫、杜云、刘陶、陈鑫爱、董霁、胡越男、陈思宇。

本文件及其所代替文件的历史版本发布情况为：

——2021年首次发布为T/TAF 077.11—2021；

——本次为第一次修订。



引 言

随着移动应用种类和数量呈爆发式增长，APP侵害用户权益事件层出不穷，个人信息保护态势愈加严峻。本文件根据《中华人民共和国个人信息保护法》等相关法律要求，依据GB/T 35273-2020《信息安全技术 个人信息安全规范》的最小必要原则，提出移动互联网应用程序在处理个人通话记录的收集、存储、使用、删除等活动中的最小必要信息规范和评估准则，旨在规范移动互联网行业，落实最小、必要的原则，促进行业的健康稳定发展。



APP 收集使用个人信息最小必要评估规范 第 11 部分：通话记录

1 范围

本文件规定了移动互联网应用程序处理终端产生的通话记录信息的最小必要评估规范,包括基本原则、信息分类、典型场景、评估要求和评估方法。

本文件适用于规范个人信息处理者通过移动互联网应用程序处理通话记录信息的活动,也适用于行业主管部门、第三方评估机构等组织对移动互联网应用程序收集使用通话记录行为进行评估。

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 35273—2020 信息安全技术 个人信息安全规范

T/TAF 077.1—2022 APP收集使用个人信息最小必要评估规范 第1部分：总则

3 术语和定义

GB/T 35273—2020和T/TAF 077.1—2022界定的以及下列术语和定义适用于本文件。

3.1

通话记录 call log

个人使用移动智能终端发起的主叫通话、被叫通话等通话行为后在终端设备内存储的通话历史信息。

3.2

个人信息处理者 personal information handler

在个人信息处理活动中自主决定个人信息处理目的、处理方式等的组织、个人。

3.3

移动互联网应用程序 mobile application software

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。

注:本文件中移动互联网应用程序指为实现个人信息处理者处理通话记录活动所运营的APP。

4 缩略语

下列缩略语适用于本文件。

APP：移动互联网应用程序(Mobile Application Software)

ID：标识(Identification)

URL：统一资源定位器(Uniform Resource Locator)

VoLTE：长期演进语音承载(Voice over Long-Term Evolution)

5 基本原则

应符合T/TAF 077.1—2022第5章的最小必要原则。

6 通话记录信息分类

通话记录信息可包括以下内容：

- 电话属性：国家代码、电话号码（例如联系人电话、个人输入电话等）、电话标记（例如受限、未知、付费等）、电话号码类型（例如工作、家庭等）、运营商地址等；
- 通话属性：通话日期、通话时长、通话形式（例如VoLTE、网络等）、双卡呼入电话号码等；
- 通话类别：呼入、呼出、未接、拦截、拒绝、外部接听等；
- 联系人属性：姓名、URL、头像ID、头像URL等；
- 未接电话原因：紧急呼叫、最大呼叫、最大接听、短铃声、音量低等；
- 电话拦截原因：未拦截、语音邮箱、未知号码、受限号码、未在通讯录、付费电话等；
- 是否已读：新记录、已读。

7 处理通话记录典型应用场景

个人信息处理者应在合理的场景下收集使用通话记录信息，以下为通过APP实现收集使用通话记录信息的典型场景：

- a) 通话处理：实现通话功能、电话增强体验及相关活动处理；
- b) 信息管理：实现搜索、优先级设置、残疾人辅助等相关功能；
- c) 通话验证：通过拨打电话进行业务验证，读通话记录中是否有相应号码确定是否接到来电；
- d) 备份/恢复：用户通话记录备份、恢复以及云端存储；
- e) 安全管理：实现骚扰/垃圾内容检测、标记、屏蔽，金融风险控制等安全相关功能；
- f) 关联设备配套应用：将移动设备与已关联设备（例如智能手表、汽车、智能家居设备等）连接起来，实现拨打/接听电话；
- g) 跨设备转移：在多个设备间（例如在手机和电脑之间）同步通话记录信息；
- h) 设备自动化：让设备根据用户设置的一个或多个条件触发条件，在操作系统的多个区域自动执行重复性操作；
- i) 车载免提使用和投影显示：与驾驶/行驶的核心功能（例如导航）直接相关的应用，尤其是在用户不方便直接操控设备的情况下需要使用的应用；
- j) 代理通话：提供中转号码以使用户拨打电话的应用。

8 评估要求

8.1 告知同意

除法律、行政法规另有规定无需向个人告知同意的情形之外，APP在处理通话记录前应满足以下告知同意要求：

- a) 应在收集通话记录前明确告知个人处理目的、方式、范围，且经个人同意后才能收集；
注：电话、通讯录、助手等终端基本功能软件本地处理通话记录信息除外，例如电话本地收集处理个人因使用终端产生的通话记录信息。
- b) 在处理通话记录的目的、方式发生变更的，应将变更部分重新告知个人，并取得个人同意后才能进行处理。

8.2 权限要求

若APP需要通过申请操作系统权限处理通话记录信息，则APP应满足以下要求：

- a) 应在具备合理应用场景前提下申请处理通话记录权限，典型场景可申请的权限见表1。若业务功能不属于典型场景，则应按照 T/TAF 077.1—2022 6.1 要求评估权限申请的必要性；
- b) 应在业务功能发生前申请相应通话记录权限，并确保个人对于申请的授权是其充分知情的前提下自愿、明确作出。

表1 典型场景可申请权限

典型场景	可申请权限	
	读通话记录	写通话记录
通话处理	✓	✓
信息管理	✓	✓
通话验证	✓	—
备份/恢复	✓	✓
安全管理	✓	✓
关联设备配套应用	✓	✓
跨设备转移	✓	✓
设备自动化	✓	✓
车载免提使用和投影显示	✓	✓
代理通话	✓	✓

8.3 收集阶段

APP收集通话记录信息应满足以下要求：

- a) 应仅限于实现处理目的所需要的最小范围收集通话记录信息，典型场景可收集的通话记录信息范围见表2。若业务功能不属于典型场景，则应按照 T/TAF 077.1—2022 6.3 要求评估收集通话记录信息必要性；
- b) 应按照满足服务需要的最低频率收集通话记录信息。

表2 典型应用场景可收集通话记录信息范围

典型场景	可收集信息范围	是否需要上传到服务器
通话处理	全部通话信息类别	否
信息管理	全部通话信息类别	否
通话验证	电话属性、通话属性、通话类别	是
备份/恢复	电话属性、通话属性、通话类别、联系人属性	是
安全管理	电话属性、通话属性、通话类别、联系人属性	是
关联设备配套应用	全部通话信息类别	否
跨设备转移	电话属性、通话属性、通话类别、联系人属性	是（云端转发模式）
		否（设备直连模式）
设备自动化	全部通话信息类别	否
车载免提使用和投影显示	全部通话信息类别	否
代理通话	全部通话信息类别	否

8.4 存储阶段

APP除备份/恢复、安全管理外，其余场景宜仅在APP客户端侧本地存储或不存储（完成功能后直接丢弃）通话记录信息，如确因业务功能需要将通话记录传输到服务器，则应在收集阶段取得个人单独同意。

8.5 使用阶段

APP使用通话记录信息应满足以下要求：

- a) APP 应严格按照告知的处理目的使用通话记录信息，若需扩大使用目的，则应在使用前按照本文件 8.1 再次进行告知同意；
- b) 不应在未取得个人同意的情况下，增加、删除、修改终端存储的通话记录信息，且不应修改信息原始内容，仅可针对信息进行排序归类、修改展现形式、添加额外字段等修改操作。

8.6 提供阶段

APP若向其它个人信息处理者提供通话记录信息，应评估接收方业务场景，仅提供满足业务需求的最小范围信息，典型场景可收集通话记录信息范围参考表2。

8.7 删除阶段

APP删除已收集的通话记录信息应满足以下要求：

- a) 超出约定的保存期限时，应删除或匿名化通话记录信息；
- b) 当个人主动申请注销服务后，应在承诺期限内删除或匿名化通话记录信息；
- c) 当APP停止运营其处理通话记录信息的服务时，应停止继续收集通话记录信息，并及时删除或匿名化通话记录信息。

9 评估方法

9.1 告知同意

评估编号	9.1.1
评估项目	8.1a)
评估要求	应在收集通话记录前明确告知个人处理目的、方式、范围，且经个人同意后才能收集。
预置条件	被测APP处于正常状态
测试步骤	a) 核查APP收集信息前是否通过隐私政策、弹窗等方式明确告知个人处理目的、方式、范围且与APP实际行为相符； b) 运行APP通话记录处理功能，检查是否收集行为在个人同意后发生。
预期结果	若以上测试步骤结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

评估编号	9.1.2
评估项目	8.1b)
评估要求	在处理通话记录的目的、方式发生变更的，应将变更部分重新告知个人，并取得个人同意后才能进行处理。
预置条件	被测APP处理通话记录的目的、方式已发生变更
测试步骤	a) 核查个人信息处理者管理规范中是否包含处理变更条款，且条款中要求变更时重新进行告知同意； b) 核查APP是否通过隐私政策、弹窗等方式将变更部分重新告知个人并征得用户同意； c) 运行APP通话记录处理功能，检查是否处理行为在个人同意后发生。
预期结果	若以上测试步骤结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

9.2 权限要求

评估编号	9.2.1
评估项目	8.2a)
评估要求	应在具备合理应用场景前提下申请处理通话记录权限。

预置条件	被测APP处于正常状态；操作系统支持处理通话记录权限申请
测试步骤	a) 核查 APP 功能是否属于典型场景且 APP 申请权限满足表 1； b) 若不属于典型场景，则按照 T/TAF 077.1—2022 7.1 评估权限申请是否满足最小必要。
预期结果	若以上测试步骤结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

评估编号	9.2.2
评估项目	8.2b)
评估要求	应在业务功能发生前申请相应通话记录权限，并确保个人对于申请的授权是其充分知情的前提下自愿、明确作出。
预置条件	被测APP处于正常状态；操作系统支持处理通话记录权限申请
测试步骤	a) 运行 APP 检查是否在处理通话记录前申请权限，并仅在个人同意后进行处理行为； b) 检查 APP 申请权限时告知是否充分，且不存在欺骗、诱导等行为。
预期结果	若以上测试步骤结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

9.3 收集阶段

评估编号	9.3.1
评估项目	8.3a)
评估要求	应仅限于实现处理目的所需要的最小范围收集通话记录信息。
预置条件	被测APP处于正常状态
测试步骤	a) 核查 APP 功能是否属于典型场景且收集传输的信息类型不超过表 2 范围； b) 若不属于典型场景，则按照 T/TAF 077.1—2022 7.3 评估收集行为是否满足最小必要。
预期结果	若以上测试步骤结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

评估编号	9.3.2
评估项目	8.3b)
评估要求	应按照满足服务需要的最低频率收集通话记录信息。
预置条件	被测APP处于正常状态
测试步骤	a) 核查 APP 收集信息频率是否为业务所必需的最低频率； b) 运行 APP，检查 APP 实际收集频率是否与业务声称的相符。
预期结果	若以上测试步骤结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

9.4 存储阶段

评估编号	9.4.1
评估项目	8.4
评估要求	APP除备份/恢复、安全管理外，其余场景宜仅在APP客户端侧本地存储或不存储（完成

	功能后直接丢弃) 通话记录信息, 如确因业务功能需要将通话记录传输到后台服务器, 则应在收集阶段取得个人单独同意。
预置条件	被测APP处于正常状态
测试步骤	a) 核查 APP 存储信息的功能, 判断是否为备份/恢复、安全管理场景; b) 若不属于以上场景, 则运行 APP 检查是否仅在客户端存储或不存储信息; c) 若不属于以上场景且 APP 服务端存储了信息, 则按照 T/TAF 077.1—2022 7.4 评估存储行为是否满足最小必要, 且 APP 是否取得了个人的单独同意。
预期结果	若以上测试步骤结果为肯定, 则测试项判定为未见异常, 否则判定为不符合要求。

9.5 使用阶段

评估编号	9.5.1
评估项目	8.5a)
评估要求	APP应严格按照告知的处理目的使用通话记录信息, 若需扩大使用目的, 则应在使用前按照本文件8.1要求再次进行告知同意。
预置条件	被测APP处于正常状态
测试步骤	a) 运行 APP, 核查 APP 使用信息的功能是否与告知内容一致; b) 若存在扩大使用目的的情况, 则核查是否再次向个人告知并征得同意。
预期结果	若以上测试步骤结果为肯定, 则测试项判定为未见异常, 否则判定为不符合要求。

评估编号	9.5.2
评估项目	8.5b)
评估要求	不应在未取得个人同意的情况下, 增加、删除、修改终端存储的通话记录信息, 且不应修改信息原始内容, 仅可针对信息进行排序归类、修改展现形式、添加额外字段等修改操作。
预置条件	被测APP具有写通话记录功能
测试步骤	a) 核查 APP 在增加、删除、修改终端通话记录信息前是否征得用户同意; b) 若存在修改行为, 则核查 APP 是否没有针对原始通话记录信息内容进行修改。
预期结果	若以上测试步骤结果为肯定, 则测试项判定为未见异常, 否则判定为不符合要求。

9.6 提供阶段

评估编号	9.6.2
评估项目	8.6
评估要求	APP若向其它个人信息处理者提供通话记录信息, 应评估接收方业务场景, 仅提供满足业务需求的最小范围信息。
预置条件	被测APP存在提供信息的行为
测试步骤	a) 核查 APP 是否在提供前对接收方进行过业务场景评估, 业务场景及提供信息范围是否满足表 2;

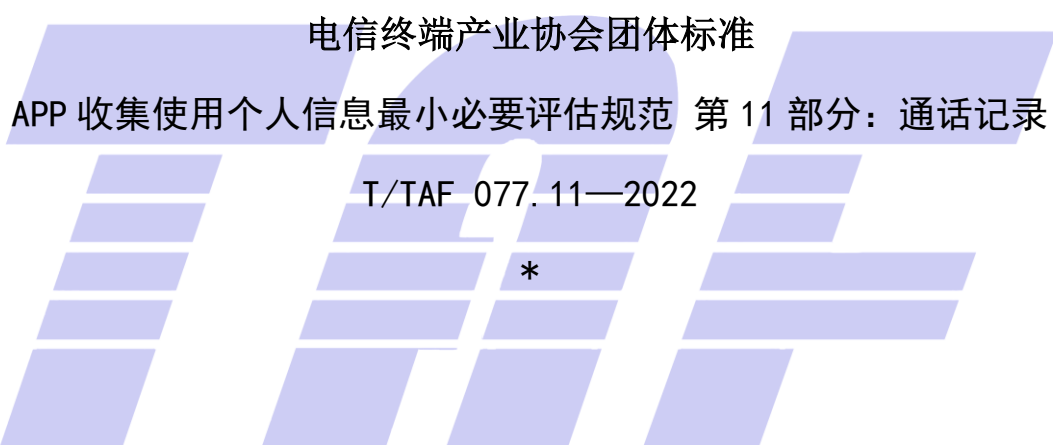
	b) 若接收方业务场景不属于表 2 典型场景, 则应按照 T/TAF 077.1—2022 7.3 评估收集信息是否必要; c) 运行 APP, 核查 APP 提供的信息是否与告知内容一致。
预期结果	若以上测试步骤结果为肯定, 则测试项判定为未见异常, 否则判定为不符合要求。

9.7 删除阶段

评估编号	9.7.1
评估项目	8.7a)
评估要求	超出约定的保存期限后, 应及时删除或匿名化通话记录信息。
前置条件	被测APP存在存储信息的行为
测试步骤	a) 核查 APP 存储信息的管理策略, 判断信息超过保存期限后, APP 是否对信息提供了必要的删除或匿名化处理。
预期结果	若以上测试步骤结果为肯定, 则测试项判定为未见异常, 否则判定为不符合要求。

评估编号	9.7.2
评估项目	8.7b)
评估要求	当个人主动申请注销服务后, 应在承诺期限内删除或匿名化通话记录信息。
前置条件	被测APP处于正常状态; 被测APP存在存储信息的行为
测试步骤	a) 运行 APP, 核查 APP 是否通过隐私政策等方式向个人明示了注销服务后对已收集的信息的处理方式; b) 核查 APP 注销服务策略, 判断注销服务后 APP 是否对信息进行了必要的删除或匿名化处理。
预期结果	若以上测试步骤结果为肯定, 则测试项判定为未见异常, 否则判定为不符合要求。

评估编号	9.7.3
评估项目	8.7c)
评估要求	当APP停止运营其处理通话记录信息的服务时, 应停止继续收集通话记录信息, 并及时删除或匿名化通话记录信息。
前置条件	被测APP已停止运营处理通话记录信息的服务; 被测APP存在存储信息的行为
测试步骤	a) 运行 APP, 核查 APP 是否通过隐私政策等方式向个人明示了服务停止后对已收集的信息的处理方式; b) 核查 APP 服务明示内容, 判断是否包含了停止服务后对信息进行停止收集、删除或匿名化处理的内容。
预期结果	若以上测试步骤结果为肯定, 则测试项判定为未见异常, 否则判定为不符合要求。



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