ICS 33.050
M 30

团　体　标　准

T/TAF 077.5-2020

APP 收集使用个人信息最小必要评估规范 设备信息

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

Device information

2020-11-26 发布　　2020-11-26 实施

电信终端产业协会　发布

目　次

前　言

本文件按照GB/T 1.1-2020的规定起草。

本文件中的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

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、北京字节跳动有限科技公司。

本文件主要起草人：王宇晓、李梦月、杨骁涵、安潇羽、高震、张吉、刘凯红、田申、宁华、王艳红。

引　言

随着移动移动互联网的迅速发展和日益成熟，移动智能终端功能的成熟与便利，设备信息已成为移动应用软件开展业务功能的重要组成部分。按照最小必要原则收集使用个人信息成为移动应用软件在个人信息处理活动中的主要目标。

本文件根据《中华人民共和国网络安全法》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，提出移动应用软件在处理涉及个人信息设备信息的收集、存储、使用、删除等活动中的最小必要信息规范和评估准则，旨在对移动互联网行业收集使用用户设备信息进行规范，落实最小、必要的原则，进一步促进移动互联网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 设备信息

1 范围

本文件规定了移动应用软件在处理涉及用户个人信息（设备信息）的收集、存储、使用、删除等活动中的最小必要评估规范，并通过设备信息在处理活动中的典型应用场景来说明如何落实最小必要原则。

本文件适用于移动应用软件提供者规范用户个人信息（设备信息）的处理活动，也适用于第三方评估机构等组织对移动应用软件收集使用设备信息行为进行监督、管理和评估。

2 规范性引用文件

下列文件对于本文件是必不可少的。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》

GB/T 35273-2020 《信息安全技术 个人信息安全规范》

T/TAF 077.1-2020《APP收集使用个人信息最小必要评估规范 总则》

3 术语和定义、缩略语

3.1 术语和定义

T/TAF 077.1-2020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

移动应用软件 mobile application

针对移动智能终端所开发的应用程序，包括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智能终端下载、安装、升级、卸载的应用软件。

3.1.3

个人信息 personal information

个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息,不包括匿名化处理后的信息。

3.1.4

个人敏感信息 personal sensitive information

一旦泄露或者非法使用,可能导致个人受到歧视或者人身、财产安全受到严重危害的个人信息,包括种族、民族、宗教信仰、个人生物特征、医疗健康、金融账户、个人行踪等信息。

3.2 缩略语

下列缩略语适用于本文件。

APP 应用软件 Application
eSIM 嵌入式SIM卡 Embedded SIM
IMEI 国际移动设备识别码 International Mobile Equipment Identity
IDFA 广告标识别符 Identifier For Advertising
IDFV 供应商标识符 Identifier For Vendor
GAID 谷歌广告标识符 Google Advertising ID
MEID 移动设备识别码 Mobile Equipment Identifier
OAID 匿名设备标识符 Open Anonymous Device Identifier

4 基本原则

应满足T/TAF 077.1-2020《APP收集使用个人信息最小必要评估规范 总则》中的最小必要原则。

5 设备信息类型

移动智能终端的设备信息类型根据其特性主要包括三类，基本设备信息、不可变设备标识、可变设备标识。

基本设备信息均为设备机型相关信息或参数，无法用于标识用户，不针对此开展最小必要性评估。

不可变设备标识在用户正常使用、系统设置或系统重置等操作发生时，不会随操作发生改变，所有应用获取到的值一致。部分终端可生成独立的不可变设备标识符，不可变设备标识的收集通常会受到系统权限机制管控。

可变设备标识在用户正常使用、系统设置或系统重置等操作行为发生时，会随行为发生改变，不同应用获取到的可能不一致。

表 1 设备信息

设备信息类别	设备信息名称
不可变设备标识	IMEI、MEID、eSIM 标识、硬件序列号、网络设备标识符等
可变设备标识	Android ID、IP 地址、IDFA、IDFV、GAID、OAID 等
基本设备信息	设备厂商名称、设备型号、CPU 型号、处理器架构、存储空间大小、设备操作系统类型、屏幕分辨率、设备名称等

6 设备信息常见收集使用场景

在移动应用中设备信息的收集使用主要用于设备识别等基础服务，再应用于具体的业务场景或服务。根据设备信息收集使用常见场景和业务类型进行分类，主要包括以下统计、推送、安全风控、个性化推荐、用户画像、支付、广告营销、日志、查找设备等。

7 个人信息处理活动各环节最小必要评估要求

7.1 收集阶段

a) 个人信息控制者在收集设备信息前应向用户告知并获得授权同意，告知同意的时机及频率应遵循最小必要原则；
b) 个人信息控制者在申请设备信息相关系统权限时，申请时机应在用户使用相关功能或服务时，用户拒绝后宜间隔 48 小时及以上再进行重新申请，用户主动申请相应功能或服务的情况除外；
c) 个人信息控制者应在保证实现相关功能或服务的前提下，按照最少必要的种类和最低频率收集设备信息。若本地处理设备信息能完成相关功能时，宜优先选择本地处理。

7.2 存储阶段

a) 设备信息的存储时间应在个人信息主体授权的存储时间或提供相关功能或服务所需的必要期限内，超出存储期限后，应及时对设备信息进行删除或匿名化处理，法律法规另有规定的除外；
b) 若法律法规或行业监管对信息保存期限另有要求，要遵守该保存期限的要求（例如物流行业）。

7.3 使用阶段

a) 设备信息的使用过程及场景应符合移动应用软件的功能或服务要求；
b) 个人信息控制者在使用相关设备信息时，应考虑到对用户的潜在影响，并尽量避免高风险的数据使用场景；
c) 对被授权访问用户设备信息的人员，应建立最小授权的访问控制策略，使其只能访问职责所需的最小必要的设备信息，且仅具备完成职责所需的最少的数据操作权限；
d) 若存在设备信息的第三方共享情况，第三方共享的设备信息类型、数量及频次不应超出业务服务的场景范围，法律法规要求的除外。

7.4 删除阶段

a) 个人信息控制者应对超出存储期限的设备信息进行删除或匿名化处理；
b) 个人信息控制者应提供途径并保证响应并实现用户删除个人信息的要求；
c) 个人信息控制者应在满足在法律规定的时限或双方约定的时间内及时响应用户删除相关个人信息的请求；如需延长答复用户的时间，应提供合理正当理由。

7.5 例外情况

a) 在某些情况下，个人信息控制者如需收集比原先预期的应用必要功能更多的个人信息，以使个人信息控制者有足够的信息来解决潜在的必要活动；
b) 在保障网络安全或运营安全的前提下，可收集不可变更的设备标识。

8 评估流程和方法

APP 收集使用人脸信息最小必要的评估流程和方法应遵循 T/TAF 077.1-2020 《APP 收集使用个人信息最小必要评估规范 总则》中的评估流程和方法。

电信终端产业协会团体标准

APP 收集使用个人信息最小必要评估规范 设备信息

T/TAF 077.5-2020

*

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