ICS 33.050
M 30

团　体　标　准

T/TAF 077.9-2021

APP 收集使用个人信息最小必要评估规范 短信信息

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

2021-01-08 发布　　2021-01-08 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《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、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、华为技术有限公司、深圳市腾讯计算机系统有限公司。

本文件主要起草人：贾科、宁华、王艳红、李腾、姚一楠、衣强。

引　　言

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短信信息的收集、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短信信息进行规范，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 短信信息

1 范围

本文件是APP收集使用个人信息最小必要评估规范系列标准中的短信信息部分，旨在贯彻个人信息收集使用的最小必要的原则，针对移动APP访问、收集、存储、使用、删除用户手机短信信息等各环节提出相应的最小必要性符合度评估项，并结合典型场景，对APP最小必要处理短信信息的进行规定。

本文件适用于规范移动互联网应用软件开发者对用户短信信息的处理，也适用于主管监管部门、第三方评估机构等组织对移动互联网应用程序收集短信信息行为进行监督、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

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、定义和缩略语

3.1 术语和定义

T/TAF 077.1-2020界定的术语和定义适用于本文件。

3.2 缩略语

下列缩略语适用于本文件。

APP 应用软件 Application

SMS 短信 Short Message

4 短信信息与必要使用场景类型

4.1 短信信息的信息类型

本文件将短信信息包含的信息类型划分为如下类型：

— 本机用户标识：用于识别或区分短信、彩信信息所在移动终端设备用户的的标识信息，可包括发送者的手机号等；依据短信信息的发送方，本机用户标识可以是短信信息的发送者标识，也可以是短信信息的接收者标识。

— 对端标识：用于识别或区分短信、彩信信息所在移动终端设备用户的的短信通信对端标识信息，包括接收者的手机号等。
— 短信内容：为短信发送者编辑并发送给接收者的各种格式的内容。单一的短信内容是否包含个人信息、包含的个人信息的类目数量以及包含的具体个人信息类型取决于每个短信内容的本身。
— 时间：移动终端设备用户接收或发送该条短信的时间。

短信信息			
本机用户标识	对端标识	短信内容	时间

4.2 典型场景类型

短信信息是移动终端用户的个人通信内容，基于多条或单条短信信息可能泄露用户隐私，甚至危害个人的人身安全和财产安全，具有较高敏感性，应在合理的场景下使用。在本文件中列举了以下七类场景为合理必要收集使用短信信息的场景：

a) 短信云备份。
以数据备份为目的，APP将用户终端上的短信信息传输至远端服务器上存储的场景。
b) 验证码便捷获取。
以协助用户完成登录或支付操作为目的，APP识别短信中的验证码并提示用户的场景。
c) 便捷短信查询与服务订阅。
以便利用户操作为目的，APP帮助用户发送特定短信指令至特定号码，查询相关信息或订阅服务的场景，如流量余额查询。
d) 短信优化编辑与发送。
以协助用户编辑并发送短信为目的，APP提供短信编辑功能并发送短信至用户指定号码的场景
e) 短信功能体验增强。
以增强用户短信功能体验为目的，APP为用户提供如短信发送商户识别和图形化展示等增强短信功能的场景
f) 手机间数据互传。
以在用户不同手机间传输数据为目的，将用户一部手机中的短信信息传输至用户另一部手机的场景，如换机。
g) 骚扰拦截。
以帮助用户拦截、屏蔽用户不期望接收的短信信息为目的，APP识别并处置相关短信信息的场景。
h) 服务智能化。
以改善服务智能化程度或用户体验为目的，APP访问用户短信信息的场景。

5 本地访问必要性评估

5.1 权限申请最小化

短信权限作为敏感权限，APP 在申请短信权限时应满足如下要求：

a) 首次启动时，若用户拒绝授权短信权限，应用不应退出或关闭。
b) APP 应基于自身业务功能和场景，以权限申请最小化为为原则，仅在业务功能触发时，向用户申请必要的短信权限；

c） 当用户拒绝短信权限时，APP 不得以退出、关闭、弹窗循环、频繁申请等方式强迫或诱导用户授权

典型场景下的 APP 可申请项如表 1 所示。

表 1 典型场景下的可申请权限

序号	典型场景	可申请权限				
		发送短信/彩信	读取短信/彩信	接收短信	写/删除短信/彩信	接收彩信
1	短信云备份	—	✓	—	✓	—
2	验证码便捷获取	—	✓	✓	—	✓
3	便捷短信查询与服务订阅	✓	—	✓	—	✓
4	短信优化编辑与发送	✓	—	—	—	—
5	短信功能体验增强	—	✓	✓	—	✓
6	手机间数据互传	—	✓	—	✓	—
7	骚扰拦截	—	✓	✓	✓	✓
8	服务智能化	—	✓	✓	✓	✓

5.2 调用行为最小化

APP在满足业务正常开展的前提下，应以最低频次调用相关短信权限，且仅访问与业务目的相关的短信信息。

本文件将短信权限的APP调用频次和时机划分为3类：

a） 用户主动触发

通过明确的用户知悉影响的动作，如点击APP交互界面上特定的按钮，触发相关行为。注：触发后，跳转到短信界面由用户进行后续操作的，不需要APP申请相应的短信权限

b） 固定周期访问

以明示并经用户确认同意的固定周期调用相关权限。

c） 短/彩信到达触发

在App已申请接收短、彩信权限时，当接收到新的短信或彩信时触发。

对于典型场景，建议的调用频次和时机如表 2 所示。

表 2 典型场景下的短信权限调用

序号	典型场景	调用频次或时机		
		发送短、彩信	读取短信/彩信	写/删除短、彩信

表2 典型场景下的短信权限调用（续）

1	云盘数据备份	—	用户主动触发 固定周期访问	用户主动触发 固定周期访问
2	验证码便捷获取	—	用户主动触发 短、彩信到达触发	—
3	便捷短信查询与服务订阅	用户主动触发	—	—
4	短信优化编辑与发送	用户主动触发	—	—
5	短信功能体验增强	—	用户主动触发 短、彩信到达触发	—
6	手机间数据互传	—	用户主动触发	用户主动触发
7	骚扰拦截	—	用户主动触发 短、彩信到达触发 固定周期访问	用户主动触发 短、彩信到达触发
8	服务智能化	—	用户主动触发 固定周期访问 短、彩信到达触发	—

6 收集使用最小必要评估

6.1 收集

6.1.1 必要收集的短信信息类型

APP服务器端需收集移动终端上用户短信信息的，应严格限定收集的短信信息类型。典型场景下，可由APP服务器端收集的短信信息类型可参考表3。

表3 典型场景下的可收集信息类型

序号	典型场景	信息类型			
		本机用户标识	对端标识	短信内容	时间
1	云端数据备份	✓	✓	✓	✓
2	验证码便捷获取	X	X	X	X

表3 典型场景下的可收集信息类型（续）

3	便捷短信查询与服务订阅	X	X	X	X
4	短信优化编辑与发送	X	X	X	X
5	短信功能体验增强	✓	X	X	✓
6	手机间数据互传	X	X	X	X
7	骚扰拦截（垃圾短信上报）	✓	✓	✓	✓
8	服务智能化	✓	X	✓	✓

6.1.2 收集范围

对于需收集短信内容的场景，APP服务器端应仅收集与业务目的相关的短信信息。

a) 云端数据备份场景下，APP 服务器端可收集终端上全量短信信息；

b) 骚扰拦截场景下，出于垃圾短信识别的目的，APP 服务端仅可在用户知情同意的前提下收集以下短、彩信信息：

1) 用户主动上报的

2) 依据用户设定的规则选定的，

3) 用户授权 APP 客户端自动识别的

c) 服务智能化场景下，仅限收集与服务目的相关的特定类别短信，或仅在特定时间段收集。

6.1.3 告知和同意

APP应在收集短信前明确告知用户短信信息收集的目的、方式、范围，经用户同意后方可收集。

6.2 存储

APP服务器端存储短信信息应满足以下要求：

a) 短信信息的存储期限应为实现个人信息主体授权使用的目的所必需的最短时间。

b) 除用户主动上报的垃圾短信外，其余场景下，应加密存储用户短信信息。

c) 在APP服务端上存储的移动终端用户的短信信息应不超过按6.1节要求评估后允许收集的短信信息的信息类型和收集范围

6.3 使用

APP服务器端使用短信信息应严格按照收集目的使用短信信息，若需扩大使用目的，则应在使用前再次告知并经个人信息主体同意后才能使用。

6.4 删除

当下述情况发生时，APP 服务器端应及时删除或匿名化处理存储的短信信息：

a) 当超出用户授权或与用户约定的存储期限后；

b) 当个人信息主体主动申请或主动注销服务后，应在承诺期限内响应在服务器端删除用户短信信息；

c) 当 APP 停止运营其收集使用短信信息的服务时。

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 短信信息

T/TAF 077.9-2021

*

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