



电信终端产业协会标准

TAF-WG4-AS0049-V1.0.0:2019

移动智能终端应用软件行为规范

Mobile Intelligent Terminal Application Software Code of Conduct

2019-12-26 发布

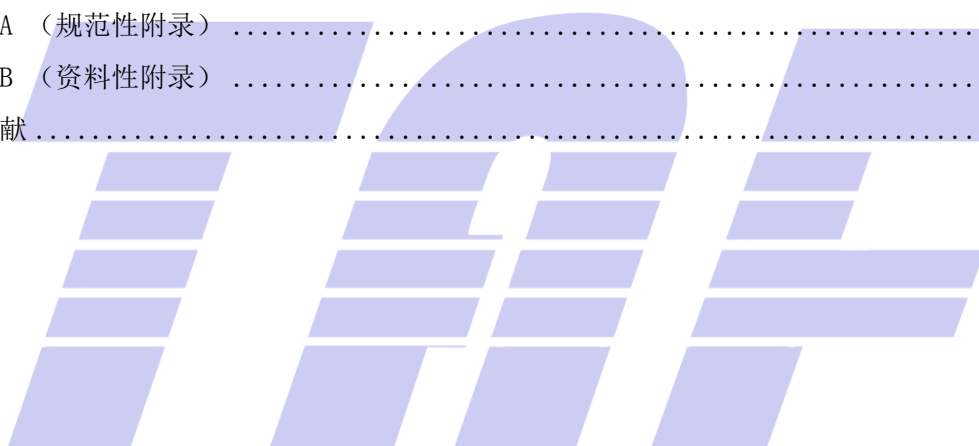
2019-12-26 实施

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	1
4 移动智能终端应用软件行为规范准则	1
4.1 基本要求	1
4.2 移动智能终端应用软件恶意行为属性	1
4.3 移动智能终端应用软件不良行为属性	6
4.4 移动智能终端应用软件不规范行为判定	8
附录 A（规范性附录）	9
附录 B（资料性附录）	10
参考文献	11



前 言

本标准按照网络安全法和GB/T 35273-2017信息安全技术-个人信息安全规范给出的规则起草。

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、广东欧泊移动通信有限公司、北京奇虎科技有限公司、北京小米科技有限责任公司。

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



引 言

移动智能终端应用软件预置和移动应用市场(商店)分发等作为应用的主要传播渠道,面向终端用户提供大量种类繁多、功能不一、形式多样的应用产品,受移动互联网时代催生,产品往往具备更为快速的迭代能力和极短的发布周期,产品的行为和安全得不到保证,而其中不乏存在浑水摸鱼的不良应用,利用与现行的法律法规打擦边球,通过损害用户个人权益的行为而获利,严重影响用户个人信息的安全。

针对应用软件行为规范的标准迫切需要出台,该标准不仅是规范移动智能终端应用软件的行为,更是为了规范移动互联网市场秩序,推动移动互联网的环境健康有序发展。本标准将适用于基于安卓操作系统的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,为我国移动智能终端与应用软件开发者提供产品行为安全规范指南,为行业市场做参考性指导。



移动智能终端应用软件行为规范

1 范围

本标准针对移动智能终端应用软件进行行为规范的要求，包括移动智能终端应用软件行为规范的基本要求、移动智能终端应用软件行为分类、移动智能终端应用软件不规范行为判定。

本标准适用于移动智能终端应用软件的行为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、升级的应用软件的行为规范。

2 规范性引用文件

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

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。

3.2 缩略语

4 移动智能终端应用软件行为规范准则

4.1 基本要求

从事移动应用分发软件/平台服务的互联网信息服务提供者，以及在移动智能终端中预置了移动应用分发平台的生产企业应对所提供的应用软件负有管理责任。

移动智能终端应用软件的行为都应遵循本规范及要求，无论该应用软件是由生产企业开发，还是由互联网信息服务提供者分发。

4.2 移动智能终端应用软件恶意行为属性

本章描述了移动智能终端应用软件所具有的恶意行为，当移动智能终端应用软件具有以下一种或多种行为时，可判定该移动智能终端应用软件具有恶意行为属性。

4.2.1 隐私盗用

在用户不知情、未明确告知或未经用户同意的情况下，获取或使用用户个人信息、工作信息或其它非公开信息的行为，具有隐私滥用行为属性。

- a) 在用户不知情、未明确告知或未经用户同意的情况下，获取或使用用户终端手机号码、其他终端身份标识（IMEI/IMSI等）；

- b) 在用户不知情、未明确告知或未经用户同意的情况下，获取或使用用户终端已安装应用软件信息的；
- c) 在用户不知情、未明确告知或未经用户同意的情况下，获取或使用用户终端运行进程信息的；
- d) 在用户不知情、未明确告知或未经用户同意的情况下，利用用户终端麦克风、摄像头等设备获取或使用图片、音频、视频信息的；
- e) 在用户不知情、未明确告知或未经用户同意的情况下，获取或使用短信内容的；
- f) 在用户不知情、未明确告知或未经用户同意的情况下，获取或使用彩信内容的；
- g) 在用户不知情、未明确告知或未经用户同意的情况下，获取或使用邮件内容的；
- h) 在用户不知情、未明确告知或未经用户同意的情况下，获取或使用通讯录内容的；
- i) 在用户不知情、未明确告知或未经用户同意的情况下，获取或使用通话记录的；
- j) 在用户不知情、未明确告知或未经用户同意的情况下，获取或使用通话内容的；
- k) 在用户不知情、未明确告知或未经用户同意的情况下，获取或使用地理位置信息的；
- l) 在用户不知情、未明确告知或未经用户同意的情况下，获取或使用用户各类帐号信息的；
- m) 在用户不知情、未明确告知或未经用户同意的情况下，获取或使用用户各类密码信息的；
- n) 在用户不知情、未明确告知或未经用户同意的情况下，获取或使用用户收藏夹信息的；
- o) 在用户不知情、未明确告知或未经用户同意的情况下，获取或使用用户文件内容的；
- p) 在用户不知情、未明确告知或未经用户同意的情况下，获取或使用用户联网信息的；
- q) 在用户不知情、未明确告知或未经用户同意的情况下，获取或使用用户网络交易信息的；
- r) 在用户不知情、未明确告知或未经用户同意的情况下，获取或使用用户下载信息的；
- s) 在用户不知情、未明确告知或未经用户同意的情况下，获取或使用用户其它个人信息的；
- t) 在用户不知情、未明确告知或未经用户同意的情况下，获取或使用用户其它工作信息的；
- u) 在用户不知情、未明确告知或未经用户同意的情况下，获取或使用其它非公开信息的。

4.2.2 过度收集

收集提供服务所必需以外的用户个人信息，具有过度收集行为属性。

移动智能终端应用软件包括但不限于具有以下任意一种行为的即具有过度收集行为属性。

- a) 收集与当前应用软件的使用场景、功能和服务不匹配的用户终端手机号码、其他终端身份标识（IMEI/IMSI等）；
- b) 收集与当前应用软件的使用场景、功能和服务不匹配的用户终端已安装应用软件信息；
- c) 收集与当前应用软件的使用场景、功能和服务不匹配的用户终端运行进程信息；
- d) 收集与当前应用软件的使用场景、功能和服务不匹配的用户终端麦克风、摄像头等设备收集图片、音频、视频信息；
- e) 收集与当前应用软件的使用场景、功能和服务不匹配的短信内容；
- f) 收集与当前应用软件的使用场景、功能和服务不匹配的彩信内容；
- g) 收集与当前应用软件的使用场景、功能和服务不匹配的邮件内容；
- h) 收集与当前应用软件的使用场景、功能和服务不匹配的通讯录内容；
- i) 收集与当前应用软件的使用场景、功能和服务不匹配的通话记录；
- j) 收集与当前应用软件的使用场景、功能和服务不匹配的通话内容；
- k) 收集与当前应用软件的使用场景、功能和服务不匹配的地理位置信息；
- l) 收集与当前应用软件的使用场景、功能和服务不匹配的用户各类帐号信息；
- m) 收集与当前应用软件的使用场景、功能和服务不匹配的用户各类密码信息；
- n) 收集与当前应用软件的使用场景、功能和服务不匹配的用户收藏夹信息；
- o) 收集与当前应用软件的使用场景、功能和服务不匹配的用户文件内容；

- p) 收集与当前应用软件的使用场景、功能和服务不匹配的用户联网信息；
- q) 收集与当前应用软件的使用场景、功能和服务不匹配的用户网络交易信息；
- r) 收集与当前应用软件的使用场景、功能和服务不匹配的用户下载信息；
- s) 收集与当前应用软件的使用场景、功能和服务不匹配的用户其它个人信息；
- t) 收集与当前应用软件的使用场景、功能和服务不匹配的用户其它工作信息；
- u) 收集与当前应用软件的使用场景、功能和服务不匹配的其它非公开信息。

4.2.3 过度使用

将收集的用户个人信息用于提供服务之外的目的，具有过度使用行为属性。

移动智能终端应用软件包括但不限于具有以下任意一种行为的即具有过度使用行为属性。

- a) 在当前应用软件提供的功能和服务不需要的场景中使用用户终端手机号码、其他终端身份标识（IMEI/IMSI 等）；
- b) 在当前应用软件提供的功能和服务不需要的场景中使用用户终端已安装应用软件信息的；
- c) 在当前应用软件提供的功能和服务不需要的场景中使用用户终端运行进程信息的；
- d) 在当前应用软件提供的功能和服务不需要的场景中利用用户终端麦克风、摄像头等设备使用图片、音频、视频信息的；
- e) 在当前应用软件提供的功能和服务不需要的场景中使用短信内容的；
- f) 在当前应用软件提供的功能和服务不需要的场景中使用彩信内容的；
- g) 在当前应用软件提供的功能和服务不需要的场景中使用邮件内容的；
- h) 在当前应用软件提供的功能和服务不需要的场景中使用通讯录内容的；
- i) 在当前应用软件提供的功能和服务不需要的场景中使用通话记录的；
- j) 在当前应用软件提供的功能和服务不需要的场景中使用通话内容的；
- k) 在当前应用软件提供的功能和服务不需要的场景中使用地理位置信息的；
- l) 在当前应用软件提供的功能和服务不需要的场景中使用用户各类帐号信息的；
- m) 在当前应用软件提供的功能和服务不需要的场景中使用用户各类密码信息的；
- n) 在当前应用软件提供的功能和服务不需要的场景中使用用户收藏夹信息的；
- o) 在当前应用软件提供的功能和服务不需要的场景中使用用户文件内容的；
- p) 在当前应用软件提供的功能和服务不需要的场景中使用用户联网信息的；
- q) 在当前应用软件提供的功能和服务不需要的场景中使用用户网络交易信息的；
- r) 在当前应用软件提供的功能和服务不需要的场景中使用用户下载信息的；
- s) 在当前应用软件提供的功能和服务不需要的场景中使用用户其它个人信息的；
- t) 在当前应用软件提供的功能和服务不需要的场景中使用用户其它工作信息的；
- u) 在当前应用软件提供的功能和服务不需要的场景中使用其它非公开信息的；
- v) 超出当前应用软件提供的功能和服务范围使用个人信息的；
- w) 超出当前应用软件提供的功能和服务范围使用工作信息的；
- x) 超出当前应用软件提供的功能和服务范围使用其他非公开信息的。

4.2.4 资费损耗

在用户不知情、未明确告知或未经用户同意的情况下，通过隐蔽运行、欺骗用户点击等方式，订购各类收费业务、自动发送短信、彩信、邮件、拨打电话、频繁连网等方式或使用移动智能终端支付，造成用户资费损失或网络虚拟财产损失等经济损失，具有资费消耗行为属性。

移动智能终端应用软件包括但不限于具有以下任意一种行为的即具有资费损耗行为属性。

- a) 在用户不知情、未明确告知或未经用户同意的情况下，自动发送短信的；
- b) 在用户不知情、未明确告知或未经用户同意的情况下，自动发送彩信的；
- c) 在用户不知情、未明确告知或未经用户同意的情况下，自动发送邮件的；
- d) 在用户不知情、未明确告知或未经用户同意的情况下，自动拨打电话的；
- e) 在用户不知情、未明确告知或未经用户同意的情况下，自动拨打收费声讯电话的；
- f) 在用户不知情、未明确告知或未经用户同意的情况下，自动订购移动增值业务的；
- g) 在用户不知情、未明确告知或未经用户同意的情况下，自动订购其它收费业务的；
- h) 在用户不知情、未明确告知或未经用户同意的情况下，自动联网的行为，5分钟时间及以内消耗流量超过统计经验值10M的阈值即判定频繁，产生异常数据流量的；
- i) 在用户不知情、未明确告知或未经用户同意的情况下，自动利用移动终端支付功能进行消费的；
- j) 在用户不知情、未明确告知或未经用户同意的情况下，自动通过其它方式扣除用户资费的；
- k) 在运行过程中存在应用收费的标准未明确提示用户；

4.2.5 远程控制

在用户不知情、未明确告知或未经用户同意的情况下，移动智能终端应用软件能够接受远程控制端指令并进行相关恶意操作的，具有远程控制行为属性。

移动智能终端应用软件包括但不限于具有以下任意一种行为的即具有远程控制行为属性。

- a) 由控制端主动向移动智能终端应用软件发起控制指令，并由终端应用软件执行从而达到不正当目的；
- b) 由控制端主动向移动智能终端应用软件推送恶意代码，并由移动智能终端应用软件加载执行的；
- c) 由移动智能终端应用软件主动向控制端请求控制指令并执行，而达到不正当目的的；
- d) 由移动智能终端应用软件主动向控制端请求恶意代码并加载执行的。

4.2.6 系统破坏

干扰、破坏、阻断移动通信网络、网络服务或其它合法业务正常运行的，通过感染、篡改、劫持、删除、终止进程等操作导致用户终端或其它非恶意软件部分或全部功能、用户文件等无法正常使用的，具有系统破坏行为属性。

移动智能终端应用软件包括但不限于具有以下任意一种行为的即具有系统破坏行为属性。

- a) 导致用户终端电池电量非正常消耗的；
- b) 导致用户终端发射功率异常的；
- c) 导致用户终端硬件无法正常工作的；
- d) 导致用户终端网络通讯功能无法正常使用的；
- e) 将可执行代码注入到其他程序的；
- f) 导致用户终端其它非恶意软件无法正常运行的；
- g) 导致其它合法业务无法正常运行的；
- h) 通过篡改系统设置、锁定用户系统等方式，导致系统无法正常运行的；
- i) 通过不合理占用系统或智能终端资源，导致终端和系统运行异常的，包括但不限于发热、卡顿；
- j) 对用户文件、系统文件或其它非恶意软件进行感染、篡改、劫持的；
- k) 除应用软件主流业务功能必须以外，诱导用户开启系统的开发者模式、USB调试模式、获取系统 root 权限的；

- l) 在用户不知情、未明确告知或未经用户同意的情况下，利用操作系统漏洞获取系统最高权限的；
- m) 在用户不知情、未明确告知或未经用户同意的情况下，对系统文件或其它非恶意软件进行删除、卸载、终止进程或限制运行的；
- n) 在用户不知情、未明确告知或未经用户同意的情况下，除应用软件合理业务功能必须以外，对用户文件进行加密的；
- o) 在用户不知情、未明确告知或未经用户同意的情况下，除应用软件合理业务功能必须以外，对用户文件进行删除的；
- p) 在用户不知情、未明确告知或未经用户同意的情况下，对系统强制锁屏的；
- q) 在用户不知情、未明确告知或未经用户同意的情况下，改变系统设置，包括但不限于音量、亮度等，影响用户正常使用的。

4.2.7 风险传播

自动通过复制、感染、投递、下载等方式将恶意应用及其衍生物进行扩散，或者通过不正当方式强制用户访问、下载、安装、付费的推广内容，或者传播色情、暴力、反动等不健康内容，具有风险传播行为属性。

移动智能终端应用软件包括但不限于具有以下任意一种行为的即具有风险传播行为属性。

- a) 在用户不知情或者未授权的情况下，诱导用户下载无关网页或安装无关应用的；
- b) 自动下载恶意应用的；
- c) 自动感染其它文件的；
- d) 自动发送包含恶意程序的彩信、邮件等；
- e) 自动发送包含恶意程序链接的短信、彩信、邮件、WAP信息等；
- f) 自动向存储卡等移动存储设备上复制恶意程序的；
- g) 自动利用有线和无线传输介质，如数据线，存储卡，蓝牙，红外等，向其它设备发送恶意程序的；
- h) 应用软件无差别地或根据地域、时段、终端机型等条件有选择地分发存在色情、暴力等违规内容的应用；
- i) 应用软件存在含有病毒、木马、恶意软件、间谍软件等侵害用户安全的行为。

4.2.8 伪造篡改

通过修改、杜撰、劫持桌面、通知、通讯录、通话记录、收藏夹、短信、彩信、邮件等方式，伪造篡改呈现给用户的信息，具有伪造篡改行为属性。

移动智能终端应用软件包括但不限于具有以下任意一种行为的即具有伪造篡改行为属性。

- a) 修改、杜撰通讯录，以诱骗用户，而达到不正当目的的；
- b) 修改、杜撰通讯记录，以诱骗用户，而达到不正当目的的；
- c) 修改、杜撰收藏夹，以诱骗用户，而达到不正当目的的；
- d) 修改、杜撰、劫持短信，以诱骗用户，而达到不正当目的的；
- e) 修改、杜撰、劫持彩信，以诱骗用户，而达到不正当目的的；
- f) 修改、杜撰、劫持邮件，以诱骗用户，而达到不正当目的的；
- g) 修改、杜撰、劫持用户文件，以诱骗用户，而达到不正当目的的；
- h) 修改、杜撰、劫持用户网络交易数据，以诱骗用户，而达到不正当目的的；

4.2.9 版权侵害

未经他人允许，直接对他人作品进行传播，或通过剽窃、杜撰、非法获取等方式将他人作品占为己有的具有版权侵害的行为，具有版权侵害行为属性。

移动智能终端应用软件包括但不限于具有以下任意一种行为的即具有版权侵害行为属性。

- a) 存在视觉可视层面的应用名称、应用内外图标等仿冒行为；
- b) 存在代码级修改层面的修改设置数据的仿冒行为；
- c) 存在代码级修改层面的清除、更换、增加广告插件的仿冒行为；
- d) 存在代码级修改层面的修改认证鉴权逻辑的仿冒行为；
- e) 存在代码级修改层面的植入恶意代码的仿冒行为；
- f) 篡改第三方应用代码或植入风险代码并发布，而达到不正当目的；
- g) 通过盗链的方式获取或使用已申明有版权的第三方的图片、音频、视频等资源；
- h) 未经他人许可，擅自对他人作品进行复制、发表、转载和传播。

4.3 移动智能终端应用软件不良行为属性

本章描述了移动智能终端应用软件所具有的不良行为，当移动智能终端应用软件具有以下一种或多种行为时，可判定该移动智能终端应用软件具有不良行为属性。

4.3.1 妨害滋扰

应用软件运行对系统没有直接损害，也不对终端用户的个人信息、资费造成侵害的其它妨害滋扰行为。

移动智能终端应用软件包括但不限于具有以下任意一种行为的即具有妨害滋扰行为属性。

- a) 在用户不知情、未明确告知或未经用户同意的情况下，在用户已经关闭应用的情况下，仍然保持后台驻留的；
- b) 在用户不知情、未明确告知或未经用户同意的情况下，长期占用移动终端中央处理器计算资源的；
- c) 在用户不知情、未明确告知或未经用户同意的情况下，通过自启动、监听事件等方式，保持应用激活，占用系统资源的；
- d) 在用户不知情、未明确告知或未经用户同意的情况下，在终端主屏幕（桌面）上增加与软件无关的图标或快捷方式的行为；
- e) 在用户不知情、未明确告知或未经用户同意的情况下，强制下载应用、可执行文件和库文件的行为；
- f) 在用户不知情、未明确告知或未经用户同意的情况下，应用软件存在静默安装和强制升级的行为；
- g) 存在反社会、反人类和政治敏感信息的；
- h) 存在违反中华人民共和国宗教相关法律法规；
- i) 存在色情、暴力和人身攻击方面内容的行为；
- j) 存在赌博、博彩方面内容的行为；
- k) 应用软件存在禁止用户卸载、制造卸载难度的行为；
- l) 应用软件存在无法正常退出的行为；
- m) 在用户未授权的情况下，执行其它违反法律法规、妨碍用户正常使用的；
- n) 通过欺骗、误导、强迫的方式或未经用户同意，通过截屏、按键记录、操作记录、日志等方式记录分析用户行为。

4.3.2 越权行为

移动智能终端应用软件在安装、运行、热更新中，存在通过强制用户授权、不合理权限申请、等越权行为。

移动智能终端应用软件包括但不限于具有以下任意一种行为的即具有越权行为属性。

- a) 应用软件权限申请时没有明确、合理的业务功能或使用场景，或申请与应用业务功能无关的其他权限的行为；
- b) 在未使用应用软件相关业务功能时，申请敏感权限或核心敏感权限的行为；
- c) 应用软件一次申请权限组中的多个权限时，未对多个权限分别列出和说明；
- d) 应用软件以默认、捆绑、停止安装使用等手段变相强迫用户授予权限申请的行为。

4.3.3 强制推广

移动智能终端应用软件通过杜撰、修改应用的显示窗口排版、系统提示窗口和控件功能，诱导终端用户点击、下载、安装、注册的强制推广行为。

移动智能终端应用软件包括但不限于具有以下任意一种行为的即具有强制推广行为属性。

- a) 应用广告存在假冒系统警告，诱导用户点击；
- b) 存在自动弹出3次及以上、占据屏幕50%及以上的广告；
- c) 存在6秒内无法关闭开屏广告；
- d) 存在广告强制用户点击；
- e) 存在应用切到后台后，仍然弹出广告；
- f) 存在应用关闭后，仍然弹出广告；
- g) 存在推送无法删除的通知栏广告，强制用户下载其他应用；
- h) 存在展示不良和违法的广告内容，包括：暴力、色情、赌博、反动等；
- i) 锁定部分应用功能，存在强制积分墙广告；
- j) 存在通过造假，欺诈等方式的变相赌博，诈骗行为的广告或功能；
- k) 应用广告伪造系统消息，存在假冒系统警告，诱导用户点击，而达到分发推广目的的；
- l) 伪造界面显示效果，诱导用户点击推广内容的；
- m) 在推送广告时，未向用户提供拒绝接收推送的选项。

4.3.4 技术滥用

移动智能终端应用软件在运行、使用过程中，未经用户允许，在非业务需求场景和用户使用情况下，进行链式启动、后台驻留、进程保活、cookie标签等技术滥用行为。

移动智能终端应用软件包括但不限于具有以下任意一种行为的即具有技术滥用属性。

- a) 应用软件运行过程中，未经用户同意的情况下，后台启动与当前应用功能和服务不相关的其他应用程序；
- b) 应用软件运行过程中，在用户不知情、未明确告知或未经用户同意，通过对终端用户的行为和个人数据进行标记并将其保存到cookie，用于用户画像的。

4.3.5 条款强制

移动智能终端应用软件在运行、使用过程中，服务协议或政策存在告知不充分、霸王条款等条款强制行为。

移动智能终端应用软件包括但不限于具有以下任意一种行为的即具有条款强制行为属性。

- a) 捆绑多项业务功能一揽子征求用户同意，不同意则不提供任何单一服务；
- b) 应用软件的服务协议要求用户授权或提供的隐私数据，除基本功能外，在用户拒绝授权或提

供的情况下，禁止用户使用；

- c) 当用户拒绝某一业务功能收集个人信息的请求时， App 停止提供其他业务功能；

4.3.6 诱骗欺诈

移动智能终端应用软件以色情、交友、博彩、中奖等失实的内容诱骗用户，而达到不正当目的的诱骗欺诈行为。

移动智能终端应用软件包括但不限于具有以下任意一种行为的即具有诱骗欺诈行为属性。

- a) 冒充国家机关、金融机构、运营商、移动终端厂商、或其它机构和个人，以诱骗用户达到不正当目的的；
- b) 伪造事实，诱骗用户退出、关闭、卸载、禁用或限制使用其它合法产品或退订服务的；
- c) 使用色情、交友、博彩等失实信息，以诱骗用户，而达到不正当目的；

4.4 移动智能终端应用软件不规范行为判定

当一个可运行于移动终端上的应用具有4.2或4.3节节所述一种或多种行为属性时，可判定为应用软件不规范行为。



附录 A
(规范性附录)
标准修订历史

修订时间	修订后版本号	修订内容



附录 B
(资料性附录)
附录



参 考 文 献

