

中华人民共和国通信行业标准

YD/T 3437—2019

移动智能终端隐私窃取恶意行为判定技术要求

**Technical requirements of privacy theft malicious behavior determination on
mobile intelligent terminal**

2019-01-25 发布

2019-07-01 实施

中华人民共和国工业和信息化部 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
4 隐私信息划分类型.....	2
5 隐私信息处理行为.....	2
5.1 收集行为.....	2
5.2 加工行为.....	2
5.3 转移行为.....	2
5.4 删除行为.....	2
6 隐私窃取恶意行为判定原则.....	2
6.1 最少必要信息原则.....	2
6.2 用户可知可控原则.....	2
6.3 隐私数据保护原则.....	2
6.4 用户主动触发原则.....	3
7 隐私窃取恶意行为等级.....	3
7.1 等级确定.....	3
7.2 判定准则.....	3
8 隐私窃取恶意行为判定方法.....	3
8.1 信息通信类.....	3
8.2 使用记录类.....	6
8.3 账户设置类.....	8
8.4 媒体影音类.....	9
8.5 传感采集类.....	11
8.6 金融支付类.....	14
8.7 设备信息类.....	16
9 隐私窃取恶意行为命名格式.....	17
9.1 隐私信息分类编码.....	17
9.2 隐私信息处理行为分类编码.....	18
9.3 命名原则.....	18
参考文献.....	19

前 言

本标准按照 GB/T 1.1-2009给出的规则起草。

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这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中国信息通信研究院、国家计算机网络应急技术处理协调中心。

本标准主要起草人：陈婉莹、潘娟、落红卫、杨正军、李媛、董霁、焦四辈、何能强。

引 言

随着移动互联网日益成熟、业务应用蓬勃发展和移动智能终端成本持续下降，移动智能终端已经成为人们日常生活必不可少的组成部分，用户真切体会到了移动智能终端带来的好处。但是，伴随业务应用在移动智能终端上广泛使用，越来越多的用户数据在移动智能终端上存储、处理和传输，其中既包括用户主动存储的个人信息，也包括业务应用在使用过程中生成的隐私数据。但是，由于移动智能终端本身的开放性和面临的严峻安全形势，这些用户数据不可避免要面临来自设备内部弱点和来自移动互联网外部攻击的双重威胁，敏感隐私用户数据泄漏以及重要个人信息丢失和损毁的事件时有发生，给用户的生活、工作和经济等多个方面带来严重影响，并最终制约了移动智能终端的健康发展。

为保护移动智能终端上的隐私信息，本标准在 YD/T 2439-2012 《移动互联网恶意程序描述格式》、YD/T 3082-2016 《移动智能终端上的个人信息保护技术要求》等标准的基础上对移动智能终端隐私窃取行为进行界定，对行为的恶意程度进行分级和评定，确保终端个人信息的机密性、完整性和可用性等安全属性。

移动智能终端隐私窃取恶意行为判定技术要求

1 范围

本标准规范了移动智能终端上的隐私信息的类型，隐私窃取恶意行为的等级，判定的原则和方法。本标准适用于移动智能终端及其安装的移动应用软件，可穿戴设备等其它类型的终端可参考使用。

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。

YD/T 2439-2012 移动互联网恶意程序描述格式

YD/T 3082-2016 移动智能终端上的个人信息保护技术要求

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。

3.1.1

移动智能终端 smart mobile terminal

能够接入移动通信网，具有能够提供应用程序开发接口的开放操作系统，并能够安装和运行第三方应用软件的移动终端。

3.1.2

隐私信息 privacy information

可为信息系统所处理、与特定自然人相关、能够单独或通过与其他信息结合识别该特定自然人的数据。

3.1.3

移动应用软件 mobile application

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

3.1.4

移动智能终端预置应用软件 pre-installed application

用户使用移动智能终端之前，已经预先装入移动智能终端的应用软件。

3.1.5

健康数据 health data

为实现疾病管理、健康健身和老龄服务等功能而需采集的人体生理指征数据。

4 隐私信息划分类型

移动智能终端隐私信息可划分为信息通信类、使用记录类、账户设置类、媒体影音类、传感采集类、金融支付类和设备信息类七种类型，具体定义见YD/T 3082-2016第4章中对移动智能终端上的个人信息类型的定义。

5 隐私信息处理行为**5.1 收集行为**

收集行为指移动智能终端对终端使用者的隐私信息进行获取并记录的过程，或移动应用软件对移动智能终端记录的隐私信息进行获取的过程，如录入通讯录、读取短信等。

5.2 加工行为

加工行为指移动智能终端或移动应用软件对终端上的隐私信息进行存储、修改、使用等过程，如存储账户密码、修改通讯录、在界面显示银行卡账号等。

5.3 转移行为

转移行为指移动智能终端或移动应用软件向终端外部传输隐私信息的过程，如向公众公开、复制到其它终端等。

5.4 删除行为

删除行为指移动智能终端或移动应用软件使终端上的隐私信息不再可用的过程，如删除浏览器历史记录、删除账号信息等。

6 隐私窃取恶意行为判定原则**6.1 最少必要信息原则**

移动智能终端收集和转移隐私信息时不得扩大隐私信息收集和转移的范围，只加工或转移与其目的有关的最少信息，达到目的后不再继续加工或转移隐私信息。

6.2 用户可知可控原则

移动智能终端对使用者要尽到告知、说明和警示的义务。以明确、易懂和适宜的方式如实向使用者告知隐私信息的收集和使用范围、加工隐私信息的目的、隐私信息转移对象、隐私信息保护措施等信息。移动智能终端主动收集、加工、转移隐私信息前要征得使用者的同意。按照告知时的承诺，不得超出范围收集、加工、转移隐私信息。

6.3 隐私数据保护原则

移动智能终端应保证加工或转移过程中隐私信息的保密、完整、可用。应采取适当的、与隐私信息遭受损害的可能性和严重性相适应的管理措施和技术手段，保护隐私信息安全，防止未经使用者授权的检索、披露及丢失、泄露、损毁和篡改隐私信息。

移动智能终端应允许用户删除终端上的隐私信息，并确保隐私信息删除的完整性和不可恢复性。

6.4 用户主动触发原则

移动智能终端收集、加工、转移、删除隐私信息应是在用户主动触发下进行，如移动智能终端需要主动收集、加工、转移隐私信息必须具有特定、明确、合理的目的，且要满足可知可控原则。

移动智能终端不可在非用户主动触发情况下删除终端上的隐私信息。

7 隐私窃取恶意行为等级

7.1 等级确定

按照隐私信息分类与每类信息可能出现的窃取行为，对移动智能终端隐私窃取行为进行判定，每种行为可从正常、风险、恶意三个级别中选择级别进行划分，如表1所示。

表1 移动智能终端隐私窃取恶意行为等级划分

	收集	加工	转移	删除
信息通信类	正常\恶意	正常\恶意	正常\风险\恶意	正常\风险\恶意
使用记录类	正常\恶意	正常\恶意	正常\风险\恶意	正常\风险
账户设置类	正常\恶意	正常\风险	正常\风险	--
媒体影音类	正常\恶意	--	正常\恶意	--
传感采集类	正常\恶意	正常\风险	正常\风险\恶意	正常\风险\恶意
金融支付类	正常\恶意	正常\风险\恶意	正常\风险\恶意	正常\风险\恶意
设备信息类	正常\恶意	--	正常\风险\恶意	--

注：“--”表示不做要求。

7.2 判定准则

根据对移动智能终端行为情况的分析，隐私窃取行为等级判断准则如下：

- 正常：移动智能终端不存在获取隐私信息的行为，或通过评测方法没有发现获取行为存在安全风险或恶意事件；
- 风险：移动智能终端存在获取隐私信息的行为，且通过评测方法发现在加工、转移隐私数据时未采取保护措施或不能彻底删除隐私数据；
- 恶意：移动智能终端存在窃取行为，且通过评测方法发现存在用户不可知可控或超出目的范围的窃取行为。

8 隐私窃取恶意行为判定方法

8.1 信息通信类

8.1.1 收集行为

判定编号：8.1.1
判定项目：信息通信类数据的收集行为

项目要求：见YD/T XXXX-XXXX 移动智能终端上的个人信息保护技术要求第8.1.1节
预制条件：被测移动智能终端处于正常工作状态
<p>判定步骤：</p> <p>步骤1：检查移动智能终端是否存在可能收集用户信息通信类数据的移动应用软件；</p> <p>步骤2：如移动智能终端存在可能收集用户信息通信类数据的移动应用软件，则运行此类软件，观察其是否存在收集用户信息通信类数据的行为；</p> <p>步骤3：如存在收集用户信息通信类数据的行为，则判断其是否向用户明示收集的目的和范围，且是在征得用户同意的情况下进行；</p> <p>步骤4：在步骤2后，如收集的用户信息通信类数据为通信录数据，则跳过步骤3，直接进行此步骤，判断是否是在提供以下服务的情况下收集通信录数据：</p> <ol style="list-style-type: none"> 1) 通信录管理、检索、备份或同步； 2) 使用通信录数据发起通信； 3) 使用通信录数据查找或推荐好友； 4) 使用通信录数据辅助快速输入； <p>步骤5：在步骤2后，如收集的用户信息通信类数据为短信/彩信数据，则跳过步骤3-步骤4，直接进行此步骤，判断是否是在提供以下服务的情况下收集短信/彩信数据：</p> <ol style="list-style-type: none"> 1) 短信/彩信管理、检索、备份或同步； 2) 垃圾短信拦截； 3) 通过短信进行业务订购或身份认证； <p>步骤6：判断收集用户信息通信类数据的移动应用软件是否有超出明示目的或范围的行为。</p>
<p>预期结果：</p> <p>在步骤2后，如移动智能终端不存在可能收集用户信息通信类数据的移动应用软件或行为，则判定等级为“正常”，判定结束；</p> <p>在步骤3后，如移动智能终端未向用户明示收集的目的和范围，或已明示收集的目的和范围但用户不可有效拒绝，则判定等级为“恶意”，判定结束；</p> <p>在步骤4后，如是在超出步骤4所列几种情况下收集通信录数据，则判定等级为“恶意”，判定结束；</p> <p>在步骤5后，如是在超出步骤5所列几种情况下收集短信/彩信数据，则判定等级为“恶意”，判定结束；</p> <p>在步骤6后，如移动智能终端不存在超出目的或范围的行为，则判定等级为“正常”，判定结束；</p> <p>在步骤6后，如移动智能终端存在超出明示目的或范围的行为，则判定等级为“恶意”，判定结束。</p>

8.1.2 加工行为

判定编号：8.1.2
判定项目：信息通信类数据的加工行为
项目要求：1、移动智能终端和移动应用软件对信息通讯类数据的修改行为应在用户主动触发的情况下进行。
预制条件：被测移动智能终端处于正常工作状态
<p>判定步骤：</p> <p>步骤1：检查移动智能终端是否存在可能修改用户信息通信类数据的移动应用软件；</p> <p>步骤2：如移动智能终端存在可能修改用户信息通信类数据的移动应用软件，则运行此类软件，观察其是否存在修改用户信息通信类数据的行为；</p> <p>步骤3：如存在加工用户信息通信类数据的行为，则判断其是否是在用户主动触发下进行的。</p>

预期结果：

在步骤2后，如移动智能终端不存在修改用户信息通信类数据的移动应用软件或行为，则判定等级为“正常”，判定结束；

在步骤3后，如是在用户主动触发下进行的，则判定等级为“正常”，判定结束；

在步骤3后，如不是在用户主动触发下进行的，则判定等级为“恶意”，判定结束。

8.1.3 转移行为

判定编号：8.1.3

判定项目：信息通信类数据的转移行为

项目要求：见YD/T XXXX-XXXX 移动智能终端上的个人信息保护技术要求第8.1.2节

预制条件：被测移动智能终端处于正常工作状态

判定步骤：

步骤1：检查移动智能终端是否存在可能转移用户信息通信类数据的移动应用软件；

步骤2：如移动智能终端存在可能转移用户信息通信类数据的移动应用软件，则运行此类软件，观察其是否存在转移用户信息通信类数据的行为；

步骤3：如存在转移用户信息通信类数据的行为，则判断其是否向用户明示转移的目的和范围，且是在征得用户同意的情况下进行；

步骤4：在步骤2后，如转移的用户信息通信类数据为通信录数据，则跳过步骤3，直接进行此步骤，判断是否是在提供以下服务的情况下转移通信录数据：

- 1) 通信录备份或同步；
- 2) 使用通信录数据查找或推荐好友；

步骤5：在步骤2后，如转移的用户信息通信类数据为短信/彩信数据，则跳过步骤3-步骤4，直接进行此步骤，判断是否是在提供以下服务的情况下转移短信/彩信数据：

- 1) 短信/彩信转发；
- 2) 短信/彩信备份或同步；
- 3) 基于云服务的垃圾短信举报或自动识别；

步骤6：判断转移用户信息通信类数据是否通过公共网络；

步骤7：如是通过公共网络转移信息通信类数据，则判断是否对数据进行加密；

步骤8：判断转移用户信息通信类数据的移动应用软件是否有超出明示目的或范围的行为。

预期结果：

在步骤2后，如移动智能终端不存在可能转移用户信息通信类数据的移动应用软件或行为，则判定等级为“正常”，判定结束；

在步骤3后，如移动智能终端未向用户明示转移的目的和范围，或已明示转移的目的和范围但用户不可有效拒绝，则判定等级为“恶意”，判定结束；

在步骤4后，如是在超出步骤4所列几种情况下转移通信录数据，则判定等级为“恶意”，判定结束；

在步骤5后，如是在超出步骤5所列几种情况下转移短信/彩信数据，则判定等级为“恶意”，判定结束；

在步骤6后，如不是通过公共网络转移信息通信类数据，则进行步骤8；

在步骤7后，如未对数据进行加密，则判定等级为“风险”，判定结束；

在步骤8后，如移动智能终端不存在超出目的或范围的行为，则判定等级为“正常”，判定结束；

在步骤8后，如移动智能终端存在超出明示目的或范围的行为，则判定等级为“恶意”，判定结束。

8.1.4 删除行为

判定编号：8.1.4
判定项目：信息通信类数据的删除行为
项目要求：1、移动智能终端或移动应用软件对信息通讯类数据的删除行为应在用户主动触发的情况下进行。 2、移动智能终端或移动应用软件应提供选项，允许用户彻底删除其保存的信息通信类数据。
预制条件：被测移动智能终端处于正常工作状态
判定步骤： 步骤1：检查移动智能终端是否存在存储信息通信类数据的能力； 步骤2：如移动智能终端存在存储信息通信类数据的能力，则运行此终端或其上的移动应用软件，观察其是否有非用户主动触发的删除行为； 步骤3：如移动智能终端没有非用户主动触发的删除行为，则检查其是否具备允许用户删除其保存的信息通信类数据的功能； 步骤4：如具备允许用户删除其保存的信息通信类数据的功能，则判断其删除是否彻底。
预期结果： 在步骤1后，如移动智能终端不存在存储信息通信类数据的能力，则判定等级为“正常”，判定结束； 在步骤2后，如移动智能终端有非用户主动触发的删除行为，则判定等级为“恶意”，判定结束； 在步骤3后，如移动智能终端不具备允许用户删除其保存的信息通信类数据的功能，则判定等级为“风险”，判定结束； 在步骤4后，如可实现彻底删除，则判定等级为“正常”，判定结束； 在步骤4后，如不可实现彻底删除，则判定等级为“风险”，判定结束。

8.2 使用记录类

8.2.1 收集行为

判定编号：8.2.1
判定项目：使用记录类数据的收集行为
项目要求：1、移动应用软件在收集移动智能终端记录的使用记录类数据前，移动应用软件应向用户明示即将进行的操作，并且仅在用户同意后方可继续。
预制条件：被测移动智能终端处于正常工作状态
判定步骤： 步骤1：检查移动智能终端是否存在可能收集用户使用记录类数据的移动应用软件； 步骤2：如移动智能终端存在可能收集用户使用记录类数据的移动应用软件，则运行此类软件，观察其是否存在收集用户使用记录类数据的行为； 步骤3：如应用存在收集用户使用记录类数据的行为，则判断其是否向用户明示收集的目的地和范围，且是在征得用户同意的情况下进行。 步骤4：判断收集用户使用记录类数据的移动应用软件是否有超出明示目的或范围的行为。
预期结果： 在步骤2后，如移动智能终端不存在收集用户使用记录类数据的移动应用软件或行为，则判定等级为“正常”，判定结束； 在步骤3后，如移动智能终端未向用户明示收集的目的地和范围，或已明示收集的目的地和范围但用户不可有效拒绝，则判定等级为“恶意”，判定结束； 在步骤4后，如移动智能终端不存在超出目的或范围的行为，则判定等级为“正常”，判定结束；

在步骤4后，如移动智能终端存在超出明示目的或范围的行为，则判定等级为“恶意”，判定结束。

8.2.2 加工行为

判定编号：8.2.2
判定项目：使用记录类数据的加工行为
项目要求：1、移动智能终端和移动应用软件不可对使用记录类数据的进行修改。
预制条件：被测移动智能终端处于正常工作状态
判定步骤： <p>步骤1：检查移动智能终端是否存在可能修改用户使用记录类数据的移动应用软件；</p> <p>步骤2：如移动智能终端存在可能修改用户使用记录类数据的移动应用软件，则运行此类软件，观察其是否存在修改用户使用记录类数据的行为。</p>
预期结果： <p>在步骤2后，如移动智能终端不存在修改用户使用记录类数据的移动应用软件或行为，则判定等级为“正常”，判定结束；</p> <p>在步骤2后，如移动智能终端存在修改用户使用记录类数据的移动应用软件或行为，则判定等级为“恶意”，判定结束。</p>

8.2.3 转移行为

判定编号：8.2.3
判定项目：使用记录类数据的转移行为
项目要求：见YD/T XXXX-XXXX 移动智能终端上的个人信息保护技术要求第8.2.1节
预制条件：被测移动智能终端处于正常工作状态
判定步骤： <p>步骤1：检查移动智能终端是否存在可能转移用户使用记录类数据的移动应用软件；</p> <p>步骤2：如移动智能终端存在可能转移用户使用记录类数据的移动应用软件，则运行此类软件，观察其是否存在转移用户使用记录类数据的行为；</p> <p>步骤3：如存在转移用户使用记录类数据的行为，则判断其是否向用户明示转移的目的和所包含隐私信息的内容，且是在征得用户同意的情况下进行；</p> <p>步骤4：判断转移用户使用记录类数据是否通过公共网络；</p> <p>步骤5：如是通过公共网络转移使用记录类数据，则判断是否对数据进行加密；</p> <p>步骤6：判断移动应用软件是否通过设置选项的方式控制使用记录类数据的转移；</p> <p>步骤7：如是通过设置选项的方式控制使用记录类数据的转移，则判断相关选项的默认设置是否为禁用使用记录类数据的转移；</p> <p>步骤8：判断转移用户使用记录类数据的移动应用软件是否有超出明示目的或所包含隐私信息的内容的行为。</p>
预期结果： <p>在步骤2后，如移动智能终端不存在可能转移用户使用记录类数据的移动应用软件或行为，则判定等级为“正常”，判定结束；</p> <p>在步骤3后，如移动智能终端未向用户明示转移的目的和和所包含隐私信息的内容，或已明示转移的目的和和所包含隐私信息的内容但用户不可有效拒绝，则判定等级为“恶意”，判定结束；</p> <p>在步骤4后，如不是通过公共网络转移使用记录类数据，则进行步骤6；</p> <p>在步骤5后，如未对数据进行加密，则判定等级为“风险”，判定结束；</p>

<p>在步骤6后，如不是通过设置选项的方式控制使用记录类数据的转移，则进行步骤8；</p> <p>在步骤7后，如未相关选项的默认设置为允许，则判定等级为“风险”，判定结束；</p> <p>在步骤8后，如移动智能终端不存在超出目的或范围的行为，则判定等级为“正常”，判定结束；</p> <p>在步骤8后，如移动智能终端存在超出明示目的或所包含隐私信息的内容的行为，则判定等级为“恶意”，判定结束。</p>

8.2.4 删除行为

判定编号：8.2.4
判定项目：使用记录类数据的删除行为
项目要求：见YD/T XXXX-XXXX 移动智能终端上的个人信息保护技术要求第8.2.2节
预制条件：被测移动智能终端处于正常工作状态
<p>判定步骤：</p> <p>步骤1：检查移动智能终端是否存在具备浏览记录和通话记录功能的移动应用软件；</p> <p>步骤2：如移动智能终端存在具备浏览记录和通话记录功能的移动应用软件，则运行此类软件，观察其是否具备允许用户删除其保存的浏览记录数据和通话记录数据的功能；</p> <p>步骤3：如具备允许用户删除其保存的浏览记录数据和通话记录数据的功能，则判断其删除是否彻底。</p>
<p>预期结果：</p> <p>在步骤1后，如移动智能终端不存在具备浏览记录和通话记录功能的移动应用软件，则判定等级为“正常”，判定结束；</p> <p>在步骤2后，如移动智能终端不具备允许用户删除其保存的浏览记录数据和通话记录数据的功能，则判定等级为“风险”，判定结束；</p> <p>在步骤3后，如可实现彻底删除，则判定等级为“正常”，判定结束；</p> <p>在步骤3后，如不可实现彻底删除，则判定等级为“风险”，判定结束。</p>

8.3 账户设置类

8.3.1 收集行为

判定编号：8.3.1
判定项目：账户设置类数据的收集行为
项目要求：1、移动应用软件不可收集移动智能终端上除本应用外的其他账户设置类数据。
预制条件：被测移动智能终端处于正常工作状态
<p>判定步骤：</p> <p>步骤1：运行移动智能终端上的移动应用软件；</p> <p>步骤2：观察是否存在有收集除本应用外的其他账户设置类数据行为的移动应用软件。</p>
<p>预期结果：</p> <p>在步骤2后，如不存在有收集除本应用外的其他账户设置类数据行为的移动应用软件，则判定等级为“正常”，判定结束；</p> <p>在步骤2后，如存在有收集除本应用外的其他账户设置类数据行为的移动应用软件，则判定等级为“恶意”，判定结束。</p>

8.3.2 加工行为

判定编号：8.3.2

判定项目：账户设置类数据的加工行为
项目要求：见YD/T XXXX-XXXX 移动智能终端上的个人信息保护技术要求第8.3.1节
预制条件：被测移动智能终端处于正常工作状态
判定步骤： <p>步骤1：检查移动智能终端是否存在可能加工用户账户设置类数据的移动应用软件；</p> <p>步骤2：如移动智能终端存在可能加工用户账户设置类数据的移动应用软件，则运行此类软件，观察其是否存在加工用户账户设置类数据的行为；</p> <p>步骤3：如存在加工用户账户设置类数据的行为，则判断其是否将认证数据中的认证凭据以密文形式存储于本地，包括但不限于数据文件、缓存文件、数据库和系统日志。</p>
预期结果： <p>在步骤2后，如移动智能终端不存在加工用户账户设置类数据的移动应用软件或行为，则判定等级为“正常”，判定结束；</p> <p>在步骤3后，如认证数据中的认证凭据以密文形式存储于本地，则判定等级为“正常”，判定结束；</p> <p>在步骤3后，如认证数据中的认证凭据以明文形式存储于本地，则判定等级为“风险”，判定结束。</p>

8.3.3 转移行为

判定编号：8.3.3
判定项目：账户设置类数据的转移行为
项目要求：见YD/T XXXX-XXXX 移动智能终端上的个人信息保护技术要求第8.3.2节
预制条件：被测移动智能终端处于正常工作状态
判定步骤： <p>步骤1：检查移动智能终端是否存在可能转移用户账户设置类数据的移动应用软件；</p> <p>步骤2：如移动智能终端存在可能转移用户账户设置类数据的移动应用软件，则运行此类软件，观察其是否存在转移用户账户设置类数据的行为；</p> <p>步骤3：如存在转移用户账户设置类数据的行为，则判断其是否通过公共网络转移用户账户设置类数据；</p> <p>步骤4：如是通过公共网络转移账户设置类数据，则判断是否对数据进行加密。</p>
预期结果： <p>在步骤2后，如移动智能终端不存在转移用户账户设置类数据的移动应用软件或行为，则判定等级为“正常”，判定结束；</p> <p>在步骤3后，如不是通过公共网络转移账户设置类数据，则判定等级为“正常”，判定结束；</p> <p>在步骤4后，如对数据进行加密，则判定等级为“正常”，判定结束。</p> <p>在步骤4后，如未对数据进行加密，则判定等级为“风险”，判定结束。</p>

8.4 媒体影音类

8.4.1 收集行为

8.4.1.1 通过摄像头的收集行为

判定编号：8.4.1.1
判定项目：媒体影音类数据通过摄像头的收集行为
项目要求：见YD/T XXXX-XXXX 移动智能终端上的个人信息保护技术要求第8.4.1节
预制条件：被测移动智能终端处于正常工作状态

判定步骤：
步骤1：检查移动智能终端是否存在可能通过摄像头收集用户媒体影音类数据的移动应用软件；
步骤2：如移动智能终端存在可能通过摄像头收集用户媒体影音类数据的移动应用软件，则运行此类软件，观察其是否存在通过摄像头收集用户媒体影音类数据的行为；
步骤3：如应用存在通过摄像头收集用户媒体影音类数据的行为，则判断其是否为手势识别、眼球跟踪、三维深度感知等需要通过摄像头收集数据、且由加工结果无法辨识原始视频图像的特殊应用；
步骤4：如应用不是手势识别、眼球跟踪、三维深度感知等需要通过摄像头收集数据、且由加工结果无法辨识原始视频图像的特殊应用，则判断是否在用户界面的显著位置通过显示图像预览的方式向用户明示即将进行的操作，且仅在用户同意后方可继续，并允许用户随时关闭数据收集；
步骤5：如应用是手势识别、眼球跟踪、三维深度感知等需要通过摄像头收集数据、且由加工结果无法辨识原始视频图像的特殊应用，则判断是否提示用户即将进行的操作，且提示的方式应为明示或使用户能够随时主动查看；
步骤6：如应用是手势识别、眼球跟踪、三维深度感知等需要通过摄像头收集数据、且由加工结果无法辨识原始视频图像的特殊应用，则判断是否提供选项允许用户打开或关闭相应功能，且开关应默认处于关闭状态。
预期结果：
在步骤2后，如移动智能终端不存在通过摄像头收集用户媒体影音类数据的移动应用软件或行为，则判定等级为“正常”，判定结束；
在步骤4后，如移动智能终端在用户界面的显著位置通过显示图像预览的方式向用户明示即将进行的操作，且仅在用户同意后方可继续，并允许用户随时关闭数据收集，则判定等级为“正常”，判定结束；
在步骤4后，如移动智能终端未在用户界面的显著位置通过显示图像预览的方式向用户明示即将进行的操作，或未在用户同意后就继续，或不允许用户随时关闭数据收集，则判定等级为“恶意”，判定结束；
在步骤5后，如未提示用户即将进行的操作，则判定等级为“恶意”，判定结束；
在步骤6后，如提供选项允许用户打开或关闭相应功能，且开关应默认处于关闭状态，则判定等级为“正常”，判定结束；
在步骤6后，如未提供选项允许用户打开或关闭相应功能，或开关默认处于开启状态，则判定等级为“恶意”，判定结束。

8.4.1.2 通过麦克风的收集行为

判定编号：8.4.1.2
判定项目：媒体影音类数据通过麦克风的收集行为
项目要求：见YD/T XXXX-XXXX 移动智能终端上的个人信息保护技术要求第8.4.1节
预制条件：被测移动智能终端处于正常工作状态
判定步骤：
步骤1：检查移动智能终端是否存在可能通过麦克风收集用户媒体影音类数据的移动应用软件；
步骤2：如移动智能终端存在可能通过麦克风收集用户媒体影音类数据的移动应用软件，则运行此类软件，观察其是否存在通过麦克风收集用户媒体影音类数据的行为；
步骤3：如应用存在通过麦克风收集用户媒体影音类数据的行为，则判断是否在用户界面的显著位置向用户明示即将进行的操作，且仅在用户同意后方可继续，并允许用户随时关闭数据收集。
预期结果：

<p>在步骤2后，如移动智能终端不存在通过麦克风收集用户媒体影音类数据的移动应用软件或行为，则判定等级为“正常”，判定结束；</p> <p>在步骤3后，如移动智能终端在用户界面的显著位置向用户明示即将进行的操作，且仅在用户同意后方可继续，并允许用户随时关闭数据收集，则判定等级为“正常”，判定结束；</p> <p>在步骤3后，如移动智能终端未在用户界面的显著位置通向用户明示即将进行的操作，或未在用户同意后就继续，或不允许用户随时关闭数据收集，则判定等级为“恶意”，判定结束。</p>
--

8.4.2 转移行为

判定编号：8.4.2
判定项目：媒体影音类数据的转移行为
项目要求：见YD/T XXXX-XXXX 移动智能终端上的个人信息保护技术要求第8.4.2节
预制条件：被测移动智能终端处于正常工作状态
<p>判定步骤：</p> <p>步骤1：检查移动智能终端是否存在可能转移用户媒体影音类数据的移动应用软件；</p> <p>步骤2：如移动智能终端存在可能转移用户媒体影音类数据的移动应用软件，则运行此类软件，观察其是否存在转移用户媒体影音类数据的行为；</p> <p>步骤3：如存在转移用户媒体影音类数据的行为，则判断其是否向用户明示即将进行的操作，并且仅在用户同意后方可继续。</p>
<p>预期结果：</p> <p>在步骤2后，如移动智能终端不存在转移用户媒体影音类数据的移动应用软件或行为，则判定等级为“正常”，判定结束；</p> <p>在步骤3后，如移动智能终端向用户明示即将进行的操作，且仅在用户同意后方可继续，则判定等级为“正常”，判定结束；</p> <p>在步骤3后，如移动智能终端未向用户明示即将进行的操作，或未在用户同意后就继续，则判定等级为“恶意”，判定结束。</p>

8.5 传感采集类

8.5.1 收集行为

判定编号：8.5.1
判定项目：传感采集类数据的收集行为
项目要求：见YD/T XXXX-XXXX 移动智能终端上的个人信息保护技术要求第8.5.1节
预制条件：被测移动智能终端处于正常工作状态
<p>判定步骤：</p> <p>步骤1：检查移动智能终端是否存在可能收集用户传感采集类数据的移动应用软件；</p> <p>步骤2：如移动智能终端存在可能收集用户传感采集类数据的移动应用软件，则运行此类软件，观察其是否存在收集用户传感采集类数据的行为；</p> <p>步骤3：如应用存在收集用户传感采集类数据的行为，则判断其是否是收集位置数据、健康数据或生物特征数据；</p> <p>步骤4：如是收集用户位置数据、健康数据，则判断其是否是在提供基于位置的服务或健康管理服务的情况下收集，并向用户明示收集的目的地和范围，且是在征得用户同意的情况下进行；</p> <p>步骤5：判断是否是持续收集用户位置数据、健康数据；</p> <p>步骤6：如是持续收集用户位置数据、健康数据，则判断其是否向用户明示进行中的收集行为，并</p>

且允许用户随时关闭数据收集；

步骤7：如是收集用户生物特征数据，则判断在执行生物特征数据的收集前，是否在用户界面的显著位置向用户明示即将进行的操作，并且仅在用户同意后方可继续。

预期结果：

在步骤2后，如移动智能终端不存在收集用户传感采集类数据的移动应用软件或行为，则判定等级为“正常”，判定结束；

在步骤4后，如移动智能终端不是在提供基于位置的服务或健康管理服务的情况下收集用户位置数据、健康数据，或未向用户明示收集的目的和范围，或已明示收集的目的和范围但用户不可有效拒绝，则判定等级为“恶意”，判定结束；

在步骤6后，如不是持续收集用户位置数据、健康数据，或向用户明示进行中的收集行为，并且允许用户随时关闭数据收集，则判定等级为“正常”，判定结束；

在步骤6后，如移动智能终端未向用户明示进行中的收集行为，或已明示进行中的收集行为但用户无法随时关闭，则判定等级为“恶意”，判定结束；

在步骤7后，如在用户界面的显著位置向用户明示即将进行的操作，并且仅在用户同意后方可继续，则判定等级为“正常”，判定结束；

在步骤7后，如未在用户界面的显著位置向用户明示即将进行的操作，或在用户界面的显著位置向用户明示即将进行的操作但用户不可有效拒绝，则判定等级为“恶意”，判定结束。

8.5.2 加工行为

判定编号：8.5.2

判定项目：传感采集类数据的加工行为

项目要求：见YD/T XXXX-XXXX 移动智能终端上的个人信息保护技术要求第8.5.2节

预制条件：被测移动智能终端处于正常工作状态

判定步骤：

步骤1：检查移动智能终端是否存在可能存储用户位置数据、健康数据和生物特征数据的移动应用软件；

步骤2：如移动智能终端存在可能存储用户位置数据、健康数据和生物特征数据的移动应用软件，则运行此类软件，观察其是否存在存储用户位置数据、健康数据和生物特征数据的行为；

步骤3：如存在存储用户位置数据、健康数据和生物特征数据的行为，则判断其是否将其存储在受保护的系统区域内，并且为其设置适当的权限，以防止未授权的访问；

步骤4：如是存储用户生物特征数据，则判断其是否是对数据进行单向变换（通常使用单向散列函数）后再进行保存。

预期结果：

在步骤2后，如移动智能终端不存在存储用户位置数据、健康数据和生物特征数据的移动应用软件或行为，则判定等级为“正常”，判定结束；

在步骤3后，如未存储在受保护的系统区域内，或存储在受保护的系统区域内但并未为其设置适当的权限，则判定等级为“风险”，判定结束；

在步骤4后，如不是存储用户生物特征数据，或对数据进行单向变换后再进行保存，则判定等级为“正常”，判定结束；

在步骤4后，如未对数据进行单向变换后再进行保存，则判定等级为“风险”，判定结束。

8.5.3 转移行为

判定编号：8.5.3
判定项目：传感采集类数据的转移行为
项目要求：见YD/T XXXX-XXXX 移动智能终端上的个人信息保护技术要求第8.5.3节
预制条件：被测移动智能终端处于正常工作状态
<p>判定步骤：</p> <p>步骤1：检查移动智能终端是否存在可能转移用户传感采集类数据的移动应用软件；</p> <p>步骤2：如移动智能终端存在可能转移用户传感采集类数据的移动应用软件，则运行此类软件，观察其是否存在转移用户传感采集类数据的行为；</p> <p>步骤3：如存在转移用户传感采集类数据的行为，则判断其是否是在提供基于位置的服务、健康管理服务或其它合理的服务场景，且相关服务的有效实现需要联网支撑的情况下，将位置数据和健康数据转移至终端外部；</p> <p>步骤4：判断移动智能终端在转移过程中是否对数据进行加密；</p> <p>步骤5：判断转移数据是否为生物特征数据；</p> <p>步骤6：如转移数据为生物特征数据，则判断是否是为了从这些信息衍生得到的其它临时认证凭据（如临时密钥）。</p>
<p>预期结果：</p> <p>在步骤2后，如移动智能终端不存在转移用户传感采集类数据的移动应用软件或行为，则判定等级为“正常”，判定结束；</p> <p>在步骤3后，如不是在提供合理的服务场景，且相关服务的有效实现不是必须在联网支撑的情况下，则判定等级为“恶意”，判定结束；</p> <p>在步骤4后，如未对数据进行加密，则判定等级为“风险”，判定结束；</p> <p>在步骤5后，如转移数据不是生物特征数据，则判定等级为“正常”，判定结束；</p> <p>在步骤6后，如是为了从这些信息衍生得到的其它临时认证凭据，则判定等级为“正常”，判定结束；</p> <p>在步骤6后，如是不为了从这些信息衍生得到的其它临时认证凭据，则判定等级为“恶意”，判定结束。</p>

8.5.4 删除行为

判定编号：8.5.4
判定项目：传感采集类数据的删除行为
项目要求：见YD/T XXXX-XXXX 移动智能终端上的个人信息保护技术要求第8.5.4节
预制条件：被测移动智能终端处于正常工作状态
<p>判定步骤：</p> <p>步骤1：检查移动智能终端是否存在可能存储用户位置数据、健康数据和生物特征数据的移动应用软件；</p> <p>步骤2：如移动智能终端存在可能存储用户位置数据、健康数据和生物特征数据的移动应用软件，则运行此类软件，观察其是否真实存储用户位置数据、健康数据和生物特征数据；</p> <p>步骤3：如存储用户位置数据、健康数据，则判断其是否允许用户删除其保存的相关信息；</p> <p>步骤4：如是存储用户生物特征数据，则判断其是否提供选项关闭生物识别功能并彻底删除操作系统存储的相关数据，且在执行此类操作前，操作系统对用户的身份进行认证。</p>
<p>预期结果：</p> <p>在步骤2后，如移动智能终端不存在存储用户位置数据、健康数据和生物特征数据的移动应用软件，</p>

则判定等级为“正常”，判定结束；

在步骤3后，如移动智能终端不允许用户删除其保存的相关信息，则判定等级为“恶意”，判定结束；

在步骤4后，如提供选项关闭生物识别功能并彻底删除操作系统存储的相关数据，且在执行此类操作前，操作系统对用户的身份进行认证，则判定等级为“正常”，判定结束；

在步骤4后，如未提供选项关闭生物识别功能，或不能删除存储的相关数据，则判定等级为“恶意”，判定结束；

在步骤4后，如不能彻底删除存储的相关数据，或在执行此类操作前操作系统未对用户的身份进行认证，则判定等级为“风险”，判定结束。

8.6 金融支付类

8.6.1 收集行为

判定编号：8.6.1
判定项目：金融支付类数据的收集行为
项目要求：见YD/T XXXX-XXXX 移动智能终端上的个人信息保护技术要求第8.6.1节
预制条件：被测移动智能终端处于正常工作状态
判定步骤： <p>步骤1：检查移动智能终端是否存在可能收集用户金融支付类数据的移动应用软件；</p> <p>步骤2：如移动智能终端存在可能收集用户金融支付类数据的移动应用软件，则运行此类软件，观察其是否存在收集用户金融支付类数据的行为；</p> <p>步骤3：如应用存在收集用户金融支付类数据的行为，则判断其是否是在提供金融支付服务或调用第三方金融支付服务的情况下，并向用户明示收集的目的地和范围，且是在征得用户同意的情况下进行。</p>
预期结果： <p>在步骤2后，如移动智能终端不存在收集用户金融支付类数据的移动应用软件或行为，则判定等级为“正常”，判定结束；</p> <p>在步骤3后，如移动智能终端是在提供提供金融支付服务或调用第三方金融支付服务的情况下收集用户金融支付类据，并向用户明示收集的目的地和范围，且是在征得用户同意的情况下进行，则判定等级为“正常”，判定结束；</p> <p>在步骤3后，如移动智能终端不是在提供提供金融支付服务或调用第三方金融支付服务的情况下收集用户金融支付类据，或未向用户明示收集的目的地和范围，或已明示收集的目的地和范围但用户不可有效拒绝，则判定等级为“恶意”，判定结束。</p>

8.6.2 加工行为

判定编号：8.6.2
判定项目：金融支付类数据的加工行为
项目要求：见YD/T 3082-2016 移动智能终端上的个人信息保护技术要求第8.6.2节
预制条件：被测移动智能终端处于正常工作状态
判定步骤： <p>步骤1：检查移动智能终端是否存在可能加工用户金融支付类数据的移动应用软件；</p> <p>步骤2：如移动智能终端存在可能加工用户金融支付类数据的移动应用软件，则运行此类软件，观察其是否存在加工用户金融支付类数据的行为；</p> <p>步骤3：如存在加工用户金融支付类数据的行为，则判断其是否是加工银行卡主账号；</p>

步骤4：如是显示银行卡主账号，则判断其是否在用户界面上显示银行卡主账号时对部分数字进行隐藏处理；

步骤5：如是存储银行卡主账号，则判断其是否在实现业务功能所必须的情况下，且存储时对账号进行加密，并为保存数据的文件设置适当的权限；

步骤6：判断移动智能终端是否在终端内部以持久性的方式存储卡片验证码、个人标识代码和卡片有效期，包括但不限于数据库、数据文件和日志记录。

预期结果：

在步骤2后，如移动智能终端不存在加工用户金融支付类数据的移动应用软件或行为，则判定等级为“正常”，判定结束；

在步骤4后，如在用户界面上显示银行卡主账号时未对部分数字进行隐藏处理，则判定等级为“风险”，判定结束；

在步骤5后，如不是在实现业务功能所必须的情况下存储银行卡主账号，则判定等级为“恶意”，判定结束；

在步骤5后，如存储时未对对账号进行加密，或未对保存数据的文件设置适当的权限，则判定等级为“风险”，判定结束；

在步骤6后，如不是在终端内部以持久性的方式存储卡片验证码、个人标识代码和卡片有效期，则判定等级为“正常”，判定结束；

在步骤6后，如在终端内部以持久性的方式存储卡片验证码、个人标识代码和卡片有效期，则判定等级为“风险”，判定结束。

8.6.3 转移行为

判定编号：8.6.3

判定项目：金融支付类数据的转移行为

项目要求：见YD/T 3082-2016 移动智能终端上的个人信息保护技术要求第8.6.3节

预制条件：被测移动智能终端处于正常工作状态

判定步骤：

步骤1：检查移动智能终端是否存在可能转移用户金融支付类数据的移动应用软件；

步骤2：如移动智能终端存在可能转移用户金融支付类数据的移动应用软件，则运行此类软件，观察其是否存在转移用户金融支付类数据的行为；

步骤3：如存在转移用户金融支付类数据的行为，则判断其是否是在执行用户支付指令时将支付信息转移至终端外部；

步骤4：判断转移的目的地是否为持有合法支付牌照的支付网关；

步骤5：如通过公共网络传输支付信息，则判断是否使用支付行业相关标准中规定的加密算法和密钥强度对数据进行加密。

预期结果：

在步骤2后，如移动智能终端不存在转移用户金融支付类数据的移动应用软件或行为，则判定等级为“正常”，判定结束；

在步骤3后，如不是在执行用户支付指令时将支付信息转移至终端外部，则判定等级为“恶意”，判定结束；

在步骤4后，如转移的目的地不是持有合法支付牌照的支付网关，则判定等级为“恶意”，判定结束；

在步骤5后，如使用支付行业相关标准中规定的加密算法和密钥强度对数据进行加密，则判定等级

为“正常”，判定结束；

在步骤5后，如未使用支付行业相关标准中规定的加密算法和密钥强度对数据进行加密，则判定等级为“风险”，判定结束。

8.6.4 删除行为

判定编号：8.6.4
判定项目：金融支付类数据的删除行为
项目要求：见YD/T 3082-2016 移动智能终端上的个人信息保护技术要求第8.6.4节
预制条件：被测移动智能终端处于正常工作状态
判定步骤： <p>步骤1：检查移动智能终端是否存在可能存储用户金融支付类数据的移动应用软件；</p> <p>步骤2：如移动智能终端存在可能存储用户金融支付类数据的移动应用软件，则运行此类软件，观察其是否真实存储用户金融支付类数据；</p> <p>步骤3：如存储用户金融支付类数据，则判断其是否允许用户删除其保存的相关信息；</p> <p>步骤4：如允许用户删除其保存的相关信息，则判断其是否使用“0”字节、“1”字节或随机字节对内存中保存相关信息的数据结构进行填充处理。</p>
预期结果： <p>在步骤2后，如移动智能终端不存在存储用户金融支付类数据的移动应用软件，则判定等级为“正常”，判定结束；</p> <p>在步骤3后，如移动智能终端不允许用户删除其保存的相关信息，则判定等级为“恶意”，判定结束；</p> <p>在步骤4后，如使用“0”字节、“1”字节或随机字节对内存中保存相关信息的数据结构进行填充处理，则判定等级为“正常”，判定结束；</p> <p>在步骤4后，如未使用“0”字节、“1”字节或随机字节对内存中保存相关信息的数据结构进行填充处理，则判定等级为“风险”，判定结束。</p>

8.7 设备信息类

8.7.1 收集行为

判定编号：8.7.1
判定项目：设备信息类数据的收集行为
项目要求：1、移动应用软件在收集移动智能终端记录的设备信息类数据前，移动应用软件应向用户明示即将进行的操作，并且仅在用户同意后方可继续。
预制条件：被测移动智能终端处于正常工作状态
判定步骤： <p>步骤1：检查移动智能终端是否存在可能收集用户设备信息类数据的移动应用软件；</p> <p>步骤2：如移动智能终端存在可能收集用户设备信息类数据的移动应用软件，则运行此类软件，观察其是否存在收集用户设备信息类数据的行为；</p> <p>步骤3：如应用存在收集用户设备信息类数据的行为，则判断其是否向用户明示收集的目的地和范围，且是在征得用户同意的情况下进行。</p> <p>步骤4：判断收集用户设备信息类数据的移动应用软件是否有超出明示目的或范围的行为。</p>
预期结果： <p>在步骤2后，如移动智能终端不存在收集用户设备信息类数据的移动应用软件或行为，则判定等级</p>

为“正常”，判定结束；
在步骤3后，如移动智能终端未向用户明示收集的目的地和范围，或已明示收集的目的地和范围但用户不可有效拒绝，则判定等级为“恶意”，判定结束；
在步骤4后，如移动智能终端不存在超出目的或范围的行为，则判定等级为“正常”，判定结束；
在步骤4后，如移动智能终端存在超出明示目的或范围的行为，则判定等级为“恶意”，判定结束。

8.7.2 转移行为

判定编号：8.7.2
判定项目：设备信息类数据的转移行为
项目要求：见YD/T 3082-2016 移动智能终端上的个人信息保护技术要求第8.7.1节
预制条件：被测移动智能终端处于正常工作状态
判定步骤： 步骤1：检查移动智能终端是否存在可能转移用户设备信息类数据的移动应用软件； 步骤2：如移动智能终端存在可能转移用户设备信息类数据的移动应用软件，则运行此类软件，观察其是否存在转移用户设备信息类数据的行为； 步骤3：如存在转移用户设备信息类数据的行为，则判断其是否向用户明示即将进行的操作，并且仅在用户同意后方可继续； 步骤4：判断移动智能终端是否是出于识别和区分用户的需要而收集设备标识信息或手机卡标识信息； 步骤5：如移动智能终端是出于识别和区分用户的需要而收集设备标识信息或手机卡标识信息，则判断在将标识信息转移出终端前是否对其进行适当的变换，使得变换后的标识信息仅适用于该应用内部识别和区分用户。
预期结果： 在步骤2后，如移动智能终端不存在转移用户媒体影音类数据的移动应用软件或行为，则判定等级为“正常”，判定结束； 在步骤3后，如移动智能终端未向用户明示即将进行的操作，或未在用户同意后就继续，则判定等级为“恶意”，判定结束； 在步骤5后，如移动智能终端在将标识信息转移出终端前对其进行适当的变换，则判定等级为“正常”，判定结束； 在步骤5后，如移动智能终端在将标识信息转移出终端前未对其进行适当的变换，则判定等级为“风险”，判定结束。

9 隐私窃取恶意行为命名格式

9.1 隐私信息分类编码

本标准将隐私信息按危害程度排序,如某恶意程序窃取多种隐私信息,则以排序靠前的属性作为主分类,以便于对其进行描述,方便公众识别。
移动互联网恶意程序属性主分类编码及排序见表 2。

表2 隐私信息分类编码

排 序	编 码	信息分类
1	Finance	金融支付类
2	Account	账户设置类

3	Sensor	传感采集类
4	Communication	信息通信类
5	Record	使用记录类
6	Media	媒体影音类
7	Device	设备信息类

9.2 隐私信息处理行为分类编码

本标准将隐私信息处理行为进行分类编码, 方便公众识别, 编码方式见表 3。

表3 隐私信息处理行为分类编码

排 序	编 码	信息分类
1	Collect	收集行为
2	Process	加工行为
3	Transfer	转移行为
4	Delete	删除行为

9.3 命名原则

见YD/T 2439-2012第4章规定的移动互联网恶意程序命名格式, 可对移动智能终端隐私窃取恶意行为命名。移动互联网恶意程序采用分段式格式命名, 前四段为必选项, 使用英文(不区分大小写)或数字标识; 第五段起为扩展字段, 扩展字段为可选项, 内容使用中括号“[]”标识, 可使用任何Unicode字符, 扩展字段可增加多个。命名格式如下:

受影响操作系统编码. 恶意程序属性主分类编码. 恶意程序名称. 变种名称. [扩展字段]

本标准所判定恶意行为的移动互联网恶意程序属性主分类编码为“privacy”, 其余字段见YD/T 2439-2012的定义。在此基础上增加隐私信息分类和处理行为信息, 具体格式如下:

受影响操作系统编码. privacy. 恶意程序名称. 变种名称. [扩展字段]. 隐私信息分类. 隐私信息处理行为

参 考 文 献

- [1] GB/Z 28828-2012 信息安全技术公共及商用服务信息系统个人信息保护指南
 - [2] YD/T 2407-2013 移动智能终端安全能力技术要求
 - [3] YD/T 2408-2013 移动智能终端安全能力测试方法
 - [4] OMA Privacy Requirements for Mobile Services V1.0
 - [5] 3GPP TR 22.949 Study on a generalized privacy capability
-