ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 41391—2022

信息安全技术　移动互联网应用程序(App)收集个人信息基本要求

Information security technology—Basic requirements for collecting personal information in mobile internet applications

2022-04-15 发布　　2022-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅲ
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 …… 3
5　App 功能划分 …… 3
6　App 收集个人信息基本要求 …… 4
6.1　最小必要收集 …… 4
6.2　必要个人信息 …… 4
6.3　特定类型个人信息 …… 5
6.4　告知同意 …… 5
6.5　系统权限 …… 6
6.6　第三方收集管理 …… 7
6.7　其他要求 …… 8
附录 A（规范性）　常见服务类型 App 必要个人信息范围及其使用要求 …… 10
附录 B（资料性）　关于 App、业务功能、必要个人信息等概念的说明 …… 22
附录 C（规范性）　特定类型个人信息收集要求 …… 24
附录 D（资料性）　可收集个人信息权限范围 …… 28
附录 E（资料性）　与常见服务类型相关程度较低的安卓系统权限 …… 32
附录 F（资料性）　常见不可变更的唯一设备识别码 …… 44
参考文献 …… 45

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。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国电子技术标准化研究院、北京理工大学、中国网络安全审查技术与认证中心、公安部第一研究所、北京信息安全测评中心、国家计算机网络应急技术处理协调中心、中国信息通信研究院、华为技术有限公司、阿里巴巴(北京)软件服务有限公司、北京百度网讯科技有限公司、蚂蚁科技集团股份有限公司、北京小桔科技有限公司、高德软件有限公司、北京字节跳动科技有限公司、北京三快科技有限公司、北京京东尚科信息技术有限公司、三六零科技集团有限公司、顺丰速运有限公司、京东科技控股股份有限公司、北京小米移动软件有限公司、北京快手科技有限公司、中国移动通信集团有限公司、贝壳找房(北京)科技有限公司、北京智者天下科技有限公司、百合佳缘网络集团股份有限公司、浙江菜鸟供应链管理有限公司、北京爱奇艺科技有限公司、中国铁道科学研究院集团有限公司铁路12306科创中心、天翼电子商务有限公司、财付通支付科技有限公司、汉庭星空(上海)酒店管理有限公司、招商银行股份有限公司、中信银行股份有限公司、中国银行股份有限公司。

本文件主要起草人：杨建军、刘贤刚、上官晓丽、胡影、周晨炜、洪延青、何延哲、刘行、陈舒、许静慧、樊华、韩煜、宋杰、李海东、刘海峰、李媛、窦禹、易立、陈湉、葛鑫、衣强、白晓媛、贾雪飞、邓婷、彭晋、张娜、徐彩曦、田申、刘笑岑、严少敏、马可、黎琳、潘景燕、张向拓、李昳婧、宜静、邱勤、张朝、门一帆、赵净、洪小崇、奚海生、杨立鹏、焦伟、史广龙、刘欣欣、王彬、封莎、陈力、何斌。

引　言

近年来，移动互联网应用程序（App）得到广泛应用，App 超范围收集、强制授权、过度索权、私自调用权限上传个人信息、敏感权限滥用等现象普遍存在，违法违规收集使用个人信息的问题突出。

本文件根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律、法规要求，重点围绕个人信息处理的最小必要原则，针对 App 违法、违规收集使用个人信息的突出问题，结合当前移动互联网技术及应用现状，在 GB/T 35273—2020《信息安全技术　个人信息安全规范》要求的基础上，给出了 App 收集个人信息应满足的基本要求，同时给出了常见服务类型 App 必要个人信息的使用要求，旨在落实《关于印发〈常见类型移动互联网应用程序必要个人信息范围规定〉的通知》（国信办秘字〔2021〕14 号）、《关于印发〈App 违法违规收集使用个人信息行为认定方法〉的通知》（国信办秘字〔2019〕191 号）等文件要求，规范 App 个人信息收集行为，最大程度地保障个人信息权益。

本文件附录 A 中常见服务类型 App 的基本业务功能、必要个人信息范围，均与《常见类型移动互联网应用程序必要个人信息范围规定》保持一致。

信息安全技术　移动互联网应用程序(App)收集个人信息基本要求

1　范围

本文件规定了App收集个人信息的基本要求,给出了常见服务类型App必要个人信息范围和使用要求。

本文件适用于App运营者规范其个人信息收集活动,也适用于监管部门、第三方评估机构等对App个人信息收集活动进行监督、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　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

3　术语和定义

GB/T 25069、GB/T 35273—2020界定的以及下列术语和定义适用于本文件。

3.1

移动互联网应用程序　mobile internet application

运行在移动智能终端上的应用程序。

注:包括移动智能终端预置、下载安装的应用程序和小程序,简称App。

3.2

移动互联网应用程序运营者　mobile internet application operator

移动互联网应用程序的所有者、管理者或提供者。

注:简称App运营者。

3.3

小程序　mini program

基于应用程序开放接口实现的,用户无需安装即可使用的移动互联网应用程序。

注:应用程序通过公开其应用程序编程接口(API)或函数,使外部的程序可以增加该应用程序的功能或使用该应用程序的资源,而不需要更改该应用程序的源代码。

3.4

业务功能　business function

满足用户具体使用目的的功能。

注:App的业务功能,可分为基本业务功能和扩展业务功能。

[来源:GB/T 35273—2020,3.17,有修改]