TC260-PG-20203A

网络安全标准实践指南

—移动互联网应用程序（App）个人信息保护常见问题及处置指南

（v1.0-202009）

全国信息安全标准化技术委员会秘书处

2020 年 9 月

本文档可从以下网址获得：
www.tc260.org.cn/

全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国信息安全标准化技术委员会（以下简称“信安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

声　明

技术支持单位

本《实践指南》得到中国电子技术标准化研究院、中国网络安全审查技术与认证中心、北京理工大学、清华大学、公安部第一研究所、北京信息安全测评中心、中国移动通信集团有限公司等单位的技术支持。

摘　要

本实践指南依据法律法规和政策标准要求，针对App存在的超范围收集、强制索权、频繁索权、未同步告知收集目的等问题，基于对相关问题出现频率的统计，给出了当前App个人信息保护十大常见问题和处置指南，建议App运营者参考本实践指南防范和处置相关问题。

目　录

1 范围

本实践指南给出了当前 App[1]个人信息保护十大常见问题及典型问题情形，同时给出了问题相应的处置建议。

本实践指南适用于 App 提供者防范和处置个人信息保护常见问题，也可为 App 开发者、移动互联网应用分发平台运营者和移动智能终端厂商提供参考。

2 App 个人信息保护十大常见问题及处置指南

2.1 未说明收集使用的个人信息目的、类型、方式

2.1.1 问题描述

App 未说明收集使用的个人信息目的、类型、方式，是指未逐一列出 App（包括委托的第三方或嵌入的第三方代码、插件）收集使用个人信息的目的、方式和范围等，其典型问题情形包括但不限于:

情形一: 使用概括性描述或不完整列举收集个人信息的业务功能及收集个人信息的目的、类型、方式。例如使用“等、例如”等方式不完整列举个人信息收集类型。

情形二: 未列出嵌入的第三方代码、插件收集使用个人信息的目的、类型、方式。App 嵌入了收集用户个人信息的第三方代码或插件（如第三方 SDK），但未通过隐私政策或其他显著方式（如第三方代码或插件隐私政策链接）向用户明示第三方代码或插件的个人信息收集使用行为。

[1] 本实践指南中的 App 是指通过预装、下载等方式获取并运行在移动智能终端上、向用户提供信息服务的应用软件。

情形三：未列出委托的第三方收集使用个人信息的目的、类型、方式。App 委托第三方进行个人信息处理，未通过隐私政策或其他方式向用户明示委托第三方的个人信息收集使用行为。

情形四：收集使用个人信息的目的、方式、范围发生变化时，未以适当方式通知用户。例如未及时更新隐私政策，或未提醒用户阅读等。

2.1.2 处置指南

该问题的处置建议，包括但不限于:

a) 完整、清晰、区分说明各业务功能所收集的个人信息。宜根据用户使用习惯逐项说明各业务功能收集个人信息的目的、类型、方式，避免使用“等、例如”等方式不完整列举。

b) 使用Cookie等同类技术（包括脚本、Clickstream、Web 信标、Flash Cookie、内嵌 Web 链接等）收集个人信息时，简要说明相关机制，以及收集个人信息的目的、类型。

c) 如嵌入的第三方代码、插件（如SDK）收集个人信息，说明第三方代码、插件的类型或名称，及收集个人信息的目的、类型、方式。

d) 如存在委托第三方处理个人信息，说明委托第三方的类型或身份、涉及的个人信息类型、委托处理目的等。

e) 收集使用个人信息的目的、方式、范围发生变化时，更新隐私政策等收集使用规则，并以推送消息、邮件、弹窗、红点提示等方式提醒用户阅读发生变化的条款。

2.2 隐私政策未征得用户明示同意

2.2.1 问题描述

App 隐私政策未征得用户明示同意，是指 App 采用默认选择同意等非明示方式征得用户同意，其典型问题情形包括但不限于:

情形一：未提示用户阅读隐私政策。未在用户首次使用或用户注册时主动提示用户阅读隐私政策，或以缩小字号、减淡颜色、遮挡等方式诱导用户略过隐私政策链接。

情形二：默认勾选同意。例如，App 在注册/登录界面下方“我已阅读并同意服务许可协议及隐私政策”前的勾选框中提前替用户打钩；注册/登录界面下方只给出隐私政策链接，并未说明注册/登录后是否视为同意隐私政策。

2.2.2 处置指南

该问题的处置建议，包括但不限于:

a) 为用户提供主动选择同意、或显著提醒用户阅读后同意隐私政策的选项，对于通过勾选框形式征得同意的，不默认勾选同意。

b) 在首次运行App或用户注册时，主动提示用户阅读隐私政策。如通过弹窗等形式主动展示隐私政策的主要或核心内容，帮助用户理解收集个人信息的范围和规则进而做出决定。

2.3 超范围收集

2.3.1 问题描述

App 超范围收集，是指违反必要原则，收集与业务功能无关的个人信息，或收集个人信息的范围、频度等超出实现 App 业务功能实

际需要，其典型问题情形包括但不限于：

情形一：收集无关个人信息。收集的个人信息类型与 App 提供的业务功能无关，例如未提供短信功能的 App 读取短信数据。

情形二：强制收集非必要个人信息。因用户不同意收集非必要个人信息，App 拒绝提供业务功能。例如：因用户拒绝提供某服务类型最小必要个人信息[2]以外的信息，App 拒绝提供该类型服务基本业务功能；仅以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，强制要求用户同意收集个人信息；在非必需的服务场景，诱导或强制采集个人生物识别信息、手持身份证照片等个人敏感信息，如可以通过密码方式验证而确保安全性的，却诱导用户使用指纹识别或人脸识别的方式验证。

情形三：过度索权。App 超范围索取权限[3]，例如：申请打开与 App 所提供业务功能无关的权限；App 安装和运行时，向用户申请当前服务类型非必要权限，用户拒绝授权申请后，App 退出、关闭或拒绝提供该类型服务基本业务功能；App 在用户未使用相关功能或服务时，提前申请开启通讯录、位置、短信、麦克风、相机等权限。

注：服务类型的必要系统权限，可参考《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范》的常见服务类型最小必要个人信息进行判断。

情形四：收集时机和频度不合理。例如：收集个人信息的频度超出 App 业务功能实际需要，特别是在静默状态或在后台运行时，收集个人信息的频度和数量超出业务需要，如预订车票功能场景下每 1

[2] 最小必要个人信息，是指保障某一服务类型正常运行最少够用的个人信息，一旦缺少将导致该服务类型基本业务功能无法实现或无法正常运行。
[3] 本实践指南中的“权限”指“可收集个人信息权限”。

秒上传一次用户精确定位信息；用户关闭 App 后，App 未经用户同意通过自启动、关联启动方式收集个人信息。

2.3.2 处置指南

该问题的处置建议，包括但不限于:

a) 结合实际的业务功能和场景所需，App收集的个人信息类型应与业务功能有直接关联，不收集与所提供业务功能无关的个人信息。

b) 遵循最小必要原则，仅申请App业务功能所必需的权限，不申请与App业务功能无关的权限（即使用户可选择拒绝）。

c) 参考《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范》，明确App所提供的服务类型和最小必要个人信息范围，且不因用户拒绝提供最小必要个人信息以外的信息，拒绝提供该类型服务的基本业务功能。

注 1：《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范》，给出了常见服务类型的最小必要个人信息。

注 2：《网络安全标准实践指南—移动互联网应用程序（App）系统权限申请使用指南》，给出了权限相关的业务功能示例，及与常见服务类型相关程度较低，不建议申请的安卓系统权限。

d) 如用户拒绝或撤回授予某服务类型非必要系统权限，App不应强制退出或关闭，且不影响与此权限无关的业务功能使用。

e) App所需的权限应在对应业务功能执行时动态申请，在用户未触发相关业务功能时，不提前申请与当前业务功能无关的权限。

f) 权限申请获得授权后，自动采集个人信息的频率应在实现App业务功能所必需的最低合理频率范围内，且仅访问满足业务功能需要的最少个人信息。

g) 除为满足法律法规规定、保护公共利益和个人重要人身财产权利之外，App开展业务活动时不应限定使用个人生物识别信息作为唯一实现业务目标的方式。

2.4 强制捆绑授权

2.4.1 问题描述

App 强制捆绑授权，是指以捆绑、频繁打扰等不合理方式征得用户同意收集个人信息或申请系统权限，其典型问题情形包括但不限于:

情形一：要求用户一次性同意打开多个可收集个人信息权限，用户不同意则无法安装或使用。例如，用户安装 App 时，以捆绑打包形式申请其向操作系统声明的所有权限，用户不同意则无法安装或使用，安装完成后申请的所有权限默认打开（如 Android 版 App 设置 targetSdkVersion 小于 23 所致）。

情形二：频繁索权。App 在用户明确拒绝权限申请后，频繁申请开启通讯录、位置、短信、麦克风、相机等与当前业务功能无关的权限骚扰用户。又如，对于用户可选提供的权限，在用户明确拒绝后，每当其重新打开 App 或进入相应界面，都会再次向用户索要或以弹窗等形式提示用户缺少相关权限，干扰用户正常使用。

情形三：以捆绑方式征得新增类型个人信息收集的同意。App 新增业务功能申请收集的个人信息超出用户原有同意范围，若用户不同意，则拒绝提供原有业务功能（新增业务功能取代原有业务功能的除外）。

2.4.2 处置指南

该问题的处置建议，包括但不限于:

a) 安卓App的目标API等级应不低于23（targetSdkVersion>=23），目标API等级宜及时更新适配安卓新版本。

注：截至本实践指南发布时，推荐设置目标 API 等级不低于 28。

b) App宜区分基本业务功能和附加业务功能，不通过捆绑服务类型、捆绑基本业务功能和附加业务功能等方式，强制要求用户一次性授权同意个人信息收集请求。

c) 对于仅为实现附加功能、个性化服务、提升用户体验，同时又并非App实现基本业务功能所必要的个人信息，可单独征得用户同意，并保障用户可拒绝个人信息收集的权利，且用户拒绝此类信息后不影响其正常使用App基本业务功能。

d) 如用户明确拒绝App业务功能所需权限，App不应频繁申请系统权限干扰用户正常使用，除非由用户主动触发功能，且没有该权限参与此业务功能无法实现。“频繁”的形式包括但不限于:

1) 单个场景在用户拒绝权限后，48小时内弹窗提示用户打开系统权限的次数超过1次;

2) 每次重新打开App或使用某一业务功能时，都会向用户索要或提示用户缺少相关系统权限。

2.5 未经用户同意收集个人信息

2.5.1 问题描述

App 未经用户同意收集个人信息，是指实际收集使用个人信息的

行为未经用户同意或违背用户意愿，其典型问题情形包括但不限于:

情形一：征得同意前开始收集个人信息。例如 App 首次运行时，用户点击同意隐私政策前已产生个人信息收集行为。

情形二：拒绝或撤回同意后仍收集个人信息。用户撤回权限授权后，仍收集相关个人信息。例如用户拒绝电话权限后，仍存在收集 IMEI 行为。

情形三：私自截留用户向第三方提供的个人信息。未经用户同意，收集用户向第三方（包括接入的第三方应用）提供的个人信息。

情形四：未征得用户同意读取剪切板或公共存储区的个人信息。如银行类 App 未在隐私政策中说明会读取剪切板内容，当用户打开银行类 App，提示用户是否向剪切板中的账号转账的情形。

情形五：私自调用权限隐蔽上传个人信息。例如，使用相机、麦克风、位置等敏感权限获取个人敏感信息时，在用户不知情情况下隐蔽读取并上传个人信息。

2.5.2 处置指南

该问题的处置建议，包括但不限于:

a) 用户点击同意隐私政策前，不产生任何个人信息收集行为。

b) 将权限申请的触发时间点置于用户点击同意隐私政策后。

c) 如App不存在下载、读取外部存储文件的实际业务功能，可直接在App自有的目录下进行保存，不建议申请外部存储权限。

d) 以下操作应由用户主动触发，并在用户知情情况下执行:

1) 执行拨打电话、发送短信等操作;

2) 打开或关闭Wi-Fi、蓝牙、GPS等;

3) 拍摄、录音、截屏、录屏等;

4) 读写用户短信、联系人等个人信息。

e) 不应隐蔽收集个人信息，当录音、拍摄、录屏、定位等敏感功能在后台执行时，应采用显著方式（如图标闪烁、状态栏提示、自定义提示条等）提示用户。

f) 不应在用户不知情或未授权的情况下，通过隐蔽方式读取并上传剪切板中包含的个人信息和公共存储区中的个人信息。

g) 对于用户直接向第三方提供个人信息的情形，不私自收集用户直接向第三方提供的个人信息。

2.6 申请权限或收集个人敏感信息未同步告知目的

2.6.1 问题描述

App 申请权限或收集个人敏感信息未同步告知目的，是指 App 申请权限或收集个人敏感信息时，未同步告知收集目的，或目的描述不明确，其典型问题情形包括但不限于:

情形一: 未同步告知个人敏感信息收集目的。收集身份证件号码、银行账户、个人生物识别信息等个人敏感信息时，未同步告知用户其目的。例如 App 收集面部识别特征前未展示单独协议或进行显著特殊说明，在用户点击“继续”后，App 在无任何提示的情况下便开始采集用户的面部识别特征。

情形二: 未告知权限申请目的。App 申请权限时未同步告知权限的申请目的，例如仅通过操作系统弹窗向用户申请权限，且未告知权

限申请目的。

情形三：目的告知不明确。目的描述不明确、难以理解，例如将目的描述为“为保证某某权限相关功能的正常使用”、“为了保证 App 正常运行”、“为了提高用户体验”等，未具体明确地说明权限的使用目的。

2.6.2 处置指南

该问题的处置建议，包括但不限于:

a) 收集个人生物识别信息前，单独向用户告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得用户的明示同意。

b) 收集身份证号、银行账户、行踪轨迹等个人敏感信息时，同步告知用户收集使用目的，目的应明确且易于理解。

c) 申请权限时应同步告知权限申请目的，目的明确且易于理解，不包含任何欺诈、诱骗、误导用户授权的描述。

d) 对于权限申请系统弹窗中可编辑目的的操作系统，App可在操作系统提供的权限申请弹窗中编辑具体明确的申请目的；权限申请系统弹窗中无法编辑目的的，建议通过App弹窗提示等方式，向用户告知权限的申请目的。

2.7 实际收集使用个人信息行为与声明不一致

2.7.1 问题描述

App 实际收集使用个人信息行为与声明不一致，是指 App 实际收集使用的个人信息超出用户授权范围，或实际行为与其所声明的隐

私政策等收集使用规则存在偏差、不一致，其典型问题情形包括但不限于：

情形一：实际收集使用个人信息的范围与隐私政策所述不一致。例如，实际收集使用个人信息范围超出隐私政策所述，即实际收集的个人信息未在隐私政策中或以其他形式说明；实际收集使用个人信息的范围少于隐私政策所述，即声明了实际并未收集的个人信息、权限或并未提供的业务功能。

情形二：故意欺瞒、掩饰收集使用个人信息的真实目的，诱骗用户同意收集个人信息或申请打开权限。例如以添加联系人为由申请通讯录权限，用户打开权限后上传整个通讯录，并将该类信息用于发送商业广告或其它目的；又如通过积分、奖励、优惠等方式欺骗误导用户提供身份证号码以及个人生物特征信息。

情形三：隐私政策所述存在明显偏差、错误。即隐私政策所述与实际情况存在明显偏差、错误，甚至出现大篇幅抄袭导致隐私政策内容不实等。

2.7.2 处置指南

该问题的处置建议，包括但不限于：

a) 实际收集的个人信息类型、申请打开可收集使用个人信息的权限、提供的业务功能等，与隐私政策等收集使用规则中相关内容一致，不超出隐私政策等收集使用规则所述范围。

b) 严格遵守隐私政策等收集使用规则，App收集或使用个人信息的功能设计同隐私政策保持一致、同步调整。

c) 明示收集使用个人信息的目的需真实、准确，不故意欺瞒、掩饰收集使用个人信息的真实目的，不诱骗用户同意收集个人信息或打开可收集个人信息权限。

2.8 未经同意向第三方提供个人信息

2.8.1 问题描述

App 未经同意向第三方提供个人信息，是指 App 未经用户同意，也未做匿名化处理，私自将其他第三方应用或服务器发送、共享个人信息，其典型问题情形包括但不限于:

情形一：App 未经同意直接向第三方提供个人信息。例如存在 App 客户端直接向第三方服务器传输个人信息（如设备识别信息、商品浏览记录、搜索使用习惯、常用软件应用列表等），或者数据传输至 App 后台服务器后，向第三方提供其收集的个人信息等行为，但未在隐私政策中说明或以其他显著方式明示用户，或未经用户授权同意，也未做匿名化处理。

情形二：内嵌 SDK 未经同意向第三方提供个人信息。例如存在嵌入的第三方代码、插件将个人信息传输至第三方服务器的行为，但未在隐私政策中说明或以其他显著方式明示用户，或未经用户授权同意，也未做匿名化处理。

2.8.2 处置指南

该问题的处置建议，包括但不限于:

a) 如存在从客户端直接向第三方发送个人信息的情形，包括通过客户端嵌入第三方代码、插件（如SDK）等方式向第三方发送个人信

息的情形，需事先征得用户同意，经匿名化处理的除外。

b) 如个人信息传输至服务器后，App运营者向第三方提供其收集的个人信息，需事先征得用户同意，经匿名化处理的除外。

c) 如向第三方传输的个人信息类型、接收数据的第三方身份等发生变更的，需以适当方式通知用户，并征得用户同意。

d) 如App接入第三方应用，当用户使用第三方应用时，需在征得用户同意后，再向第三方应用提供个人信息。当用户获知应用为第三方提供后，自行以主动填写等方式向第三方直接授权的除外。

e) App提供者宜对于接入的第三方应用收集个人信息的合法、正当、必要性等方面进行审核，并明确标识相关业务功能为第三方提供。

f) 用户跳转至第三方应用时，宜提醒用户关注第三方应用的收集使用规则。

g) App宜对第三方代码（如SDK）使用的权限进行审核，要求引入第三方代码所需使用的权限最小化。

h) App宜采取技术检测、安全审计等手段，确保第三方代码或插件收集、使用行为符合约定要求。

2.9 未提供删除、更正或投诉举报的功能或渠道

2.9.1 问题描述

App 未提供删除、更正或投诉举报的功能或渠道，是指 App 未提供有效且能及时响应的删除、更正或投诉举报的功能或渠道，或设置不合理条件，其典型问题情形包括但不限于：

情形一：无法删除个人信息或设置不合理条件。例如，App 未提

供有效的个人信息删除功能或渠道；为删除个人信息设置不合理条件；未按相关要求或约定时限响应用户删除个人信息请求等。

情形二：无法更正个人信息或设置不合理条件。例如，App 未提供有效的个人信息更正功能或渠道；为更正个人信息设置不合理条件；未按相关要求或约定时限响应用户更正个人信息请求；用户已完成更正个人信息操作，但 App 后台并未完成的等。

情形三：未提供个人信息申诉渠道或用户申诉机制无效。例如，未建立并公布个人信息安全投诉、举报渠道，或未在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）受理并处理的。

2.9.2 处置指南

该问题的处置建议，包括但不限于:

a) 提供有效的更正、删除个人信息的途径。

b) 宜提供在线操作方式及时响应个人信息更正、删除请求，需人工处理的，应在承诺时限内（承诺时限不得超过15个工作日，无承诺时限的，以15个工作日为限）完成核查和处理。

c) 更正和删除个人信息的功能应简单易操作，不设置不必要或不合理的条件。

d) 用户更正、删除个人信息等操作完成时，App后台及时执行完成相关操作，因法律法规规定需要留存个人信息的，不再将其用于日常业务中。

e) 建立并公布可受理个人信息安全问题相关的投诉、举报渠道，

受理可采取在线操作、客服电话、电子邮件等方式。

f) 妥善受理用户关于个人信息相关的投诉、举报，并在承诺时限内（承诺时限不得超过15个工作日，无承诺时限的，以15个工作日为限）受理并处理。

2.10 未提供有效的注销用户账号途径

2.10.1 问题描述

App 未提供有效的注销用户账号途径，是指 App 未提供有效的注销用户账号功能或渠道，或为注销用户账号设置不必要或不合理条件，其典型问题情形包括但不限于：

情形一：无法注销或未按要求注销。例如：App 未提供注销用户账号的功能或渠道；通过 App 界面、邮件、客服电话等渠道提交注销申请后，未按相关要求或约定完成注销；受理注销账户请求后，未在承诺时限内（不超过 15 个工作日）完成核查和处理；注销成功后，未按相关要求或约定对用户个人信息进行删除或匿名化处理（法律法规另有规定的除外）；用户难以找到注销入口，或注销操作流程非常复杂不易操作等。

情形二：设置不合理的注销账号条件。例如：注销过程进行身份核验时，要求用户提交超过 App 注册、使用时收集的个人信息类型（如注册使用时未提供身份信息，但是注销时要求提供手持身份证照片、绑定银行卡等）；对于采用同一账号注册登录多个 App 的情形，注销或退出单个 App 将导致其他无必要业务关联的 App 不能使用；要求用户填写精确的历史操作记录作为注销的必要条件等。

2.10.2 处置指南

该问题的处置建议，包括但不限于:

a) 提供简便易操作的注销功能或渠道，若有可能宜在应用或网站上设置便捷的交互页面提供在线注销功能，且注销入口易于访问，注销状态易于查询。

b) 不设置不合理的注销条件，不响应账号注销请求的情形不超过GB/T 35273-2020《信息安全技术 个人信息安全规范》8.7 e）给出的情形。

注：如用户自愿选择放弃账号下相应权益（如XX币、XX积分），若有可能宜允许用户注销账号。

c) 注销过程如需进行身份核验，不要求用户提供超出注册、使用等服务环节收集的个人信息类型，特别是注销时要求额外提供手持身份证照片、银行卡绑定、人脸识别等。

d) 制定并公开账号注销条款，明示账号注销的条件、后果、方法、流程等信息。

注：注销条款可作为个人信息保护政策的章节，也可制定单独的注销协议。

e) 及时响应用户注销请求，需要人工处理的，在承诺时限内（不超过15个工作日）完成核查和处理。

f) 用户注销后的数据处理，建议:

1) 注销后停止对用户个人信息的收集和使用，并按照相关要求和约定删除其个人信息或匿名化处理;

2) 因法律法规规定需要留存个人信息的，将其隔离存储，不再将其用于日常业务活动中;

3) 注销时因验证用户身份所收集的个人敏感信息，完成用户身份验证后立即删除或匿名化处理。

g) 多个App共用一个账号体系时，单个App注销建议：

1) 用户可退出或注销单个App，且不影响无必要业务关联App的正常使用；

2) 提供解除单个App用户账号使用关系等措施实现注销，并对该App账号以外其他个人信息进行删除；

3) 如多个App之间存在必要业务关联而无法拆分账号，需在注销前向用户详细说明账号关联的应用、注销条件、注销后果等信息。

注：存在必要业务关联，是指如一旦注销某个 App 的账号，将会导致其他 App 的必要业务功能无法实现或者服务质量明显下降的。

参考文献

[1] 国家标准《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范》（征求意见稿）. 2020-01-20.

[2] 中国电子技术标准化研究院. App 个人信息保护合规十大常见问题及处置策略. 2019-10-25.

[3] App 专项治理工作组. App 申请权限时告知目的，是多此一举吗？. 2019-06-25.