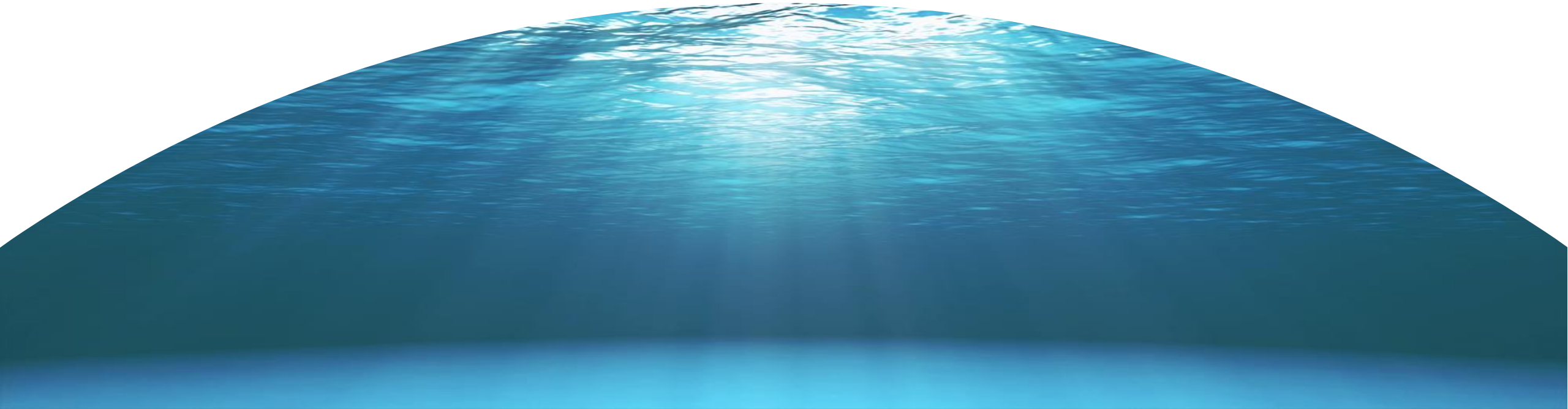
移动APP合规性解决方案

海云安 secidea

安 全 每 一 行 代 码

ideas for code security



目录
CONTENTS

01 需 求 背 景
Requirements Introduction

02 解 决 方 案
Product Solutions

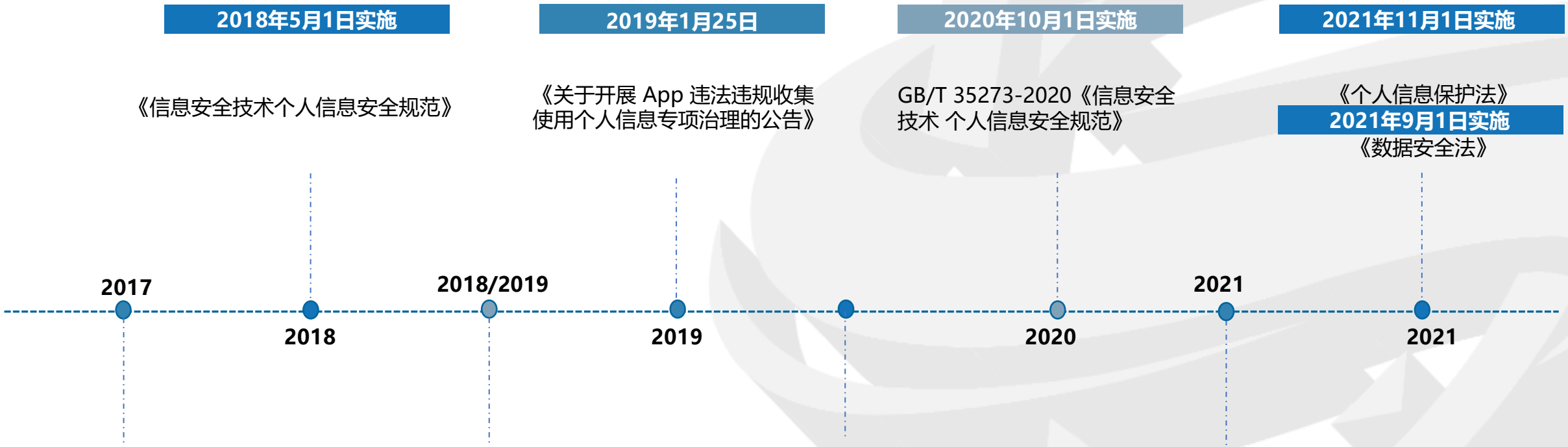
03 服 务 内 容
Services Content

海云安
secidea

PART01

需求背景

法律法规相继出台



2017年6月1日实施

《中华人民共和国网络安全法》

2018年5月1日实施

《信息安全技术个人信息安全规范》

2018年11月发布

《电信和互联网用户个人信息保护白皮书》

2019年1月25日

《关于开展 App 违法违规收集使用个人信息专项治理的公告》

2019年12月1日

GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》
《信息安全技术 网络安全等级保护基本要求 第 3 部分：移动互联安全扩展要求》

2020年10月1日实施

GB/T 35273-2020《信息安全技术 个人信息安全规范》

2021年5月1日实施

四部门联合发布《常见类型移动互联网应用程序必要个人信息范围规定》

2021年11月1日实施

《个人信息保护法》

2021年9月1日实施

《数据安全法》

工信部开展专项整治活动

工业和信息化部关于开展纵深推进APP侵害用户权益专项整治行动的通知

发布时间：2020-07-24 来源：信息通信管理局 分享：

工信部信管函（2020）164号

各省、自治区、直辖市通信管理局，中国信息通信研究院、中国互联网协会，各相关单位：

按照2020年信息通信行业行风建设暨纠风工作部署，为切实加强用户个人信息保护，为人民群众提供更安全、更健康、更干净的信息环境，我部决定开展纵深推进APP侵害用户权益专项整治行动。专项整治时间为通知印发之日至2020年12月10日。具体事项通知如下：

一、整治目标

依据《网络安全法》、《电信条例》、《规范互联网信息服务市场秩序若干规定》（工业和信息化部令第20号）、《电信和互联网用户个人信息保护规定》（工业和信息化部令第24号）和《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407号）等规定，深入推进技管结合，加强监督检查，督促相关企业强化APP个人信息保护，及时整改消除违规收集、使用用户个人信息和骚扰用户、欺骗误导用户、应用分发平台管理责任落实不到位等突出问题，净化APP应用空间。2020年8月底前上线运行全国APP技术检测平台管理系统，12月10日前完成覆盖40万款主流APP检测工作。

二、整治对象

（一）APP服务提供者，即互联网信息服务提供者提供的可以下载、安装、升级的应用软件，包括快应用和小程序等新应用形态。

（二）软件工具开发包（SDK）提供者，即集成在手机APP里的第三方工具集合。

（三）应用分发平台，包括网站、应用商店、APP等承担下载、安装、升级等分发服务的各类平台。

三、整治任务

（一）APP、SDK违规处理用户个人信息方面。

1. 违规收集个人信息。重点整治APP、SDK未告知用户收集个人信息的目的、方式、范围且未经用户同意，私自收集用户个人信息的行为。

2. 超范围收集个人信息。重点整治APP、SDK非服务所必需或无合理应用场景，特别是在静默状态下或在后台运行时，超范围收集个人信息的行为。

3. 违规使用个人信息。重点整治APP、SDK未向用户告知且未经用户同意，私自使用个人信息，将用户个人信息用于其提供服务之外的目的，特别是私自向其他应用或服务器发送、共享用户个人信息的行为。

4. 强制用户使用定向推送功能。重点整治APP、SDK未以显著方式标示且未经用户同意，将收集到的用户搜索、浏览记录、使用习惯等个人信息，用于定向推送或广告精准营销，且未提供关闭该功能选项的行为。

工信部个人信息安全检查流程

常规抽查

↓

第一次检查不通过

↓

通知APP开发者在规定时间内整改（10个工作日）

↓

第二次检查不通过

↓

通报并下架

网信办针对个人信息安全保护检查

九、工作要求

针对检测发现的问题，相关App运营者应当于本通报发布之日起15个工作日内完成整改，并将整改报告加盖公章发至电子邮箱：Appzhili@cac.gov.cn。各地网信办指导督促本地区App运营者按要求限期进行整改。逾期未完成整改的我办将依法予以处置。

联系电话：010-55635853

国家互联网信息办公室

2021年6月11日

网信办个人信息安全检查流程

常规抽查

↓

第一次检查不通过

↓

通知APP开发者在规定时间内整改（15个工作日）

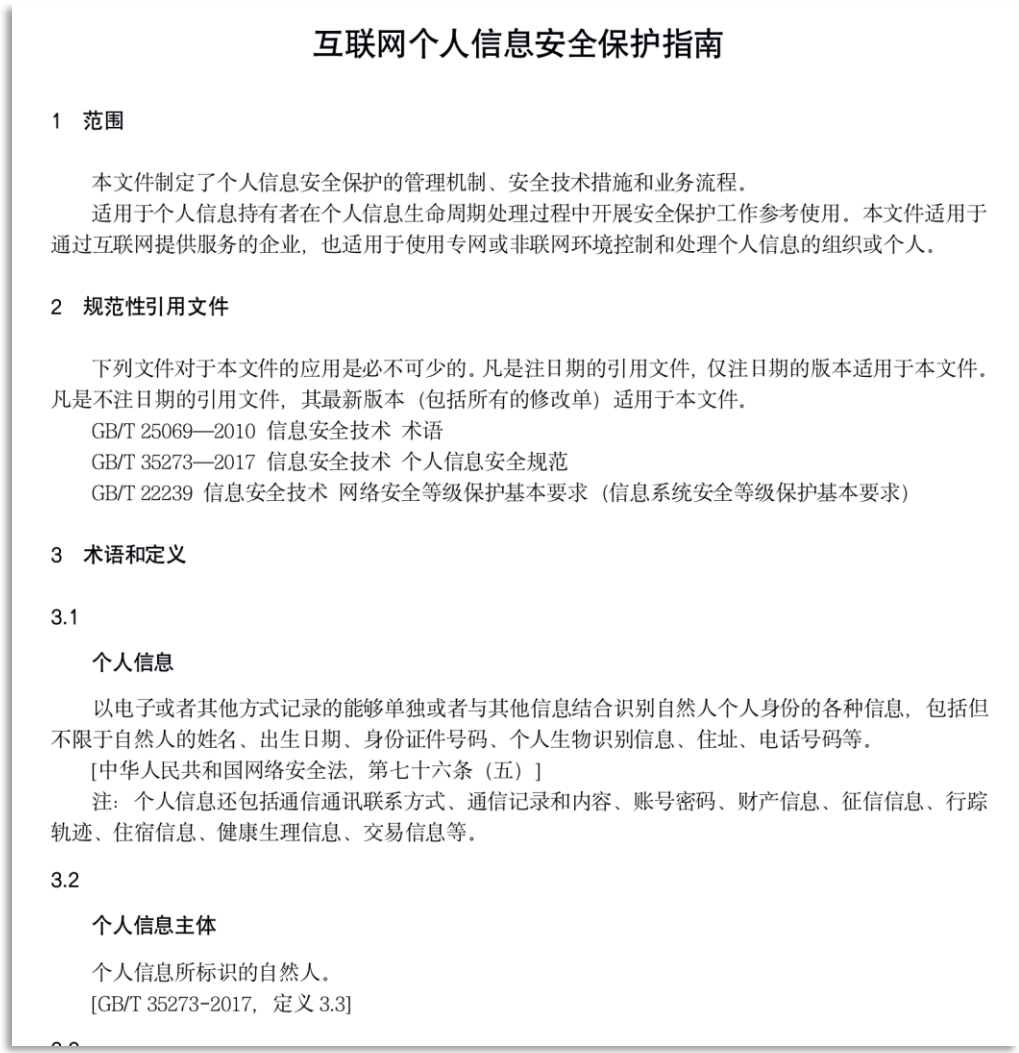
↓

第二次检查不通过

↓

依法采取通知下架、停止接入等措施给予行政处罚

公安部针对个人信息安全保护检查



互联网个人信息安全保护指南

1 范围

本文件制定了个人信息安全保护的管理机制、安全技术措施和业务流程。

适用于个人信息持有者在个人信息生命周期处理过程中开展安全保护工作参考使用。本文件适用于通过互联网提供服务的企业，也适用于使用专网或非联网环境控制和处理个人信息的组织或个人。

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。

GB/T 25069—2010 信息安全技术 术语

GB/T 35273—2017 信息安全技术 个人信息安全规范

GB/T 22239 信息安全技术 网络安全等级保护基本要求（信息系统安全等级保护基本要求）

3 术语和定义

3.1

个人信息

以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

[中华人民共和国网络安全法，第七十六条（五）]

注：个人信息还包括通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

3.2

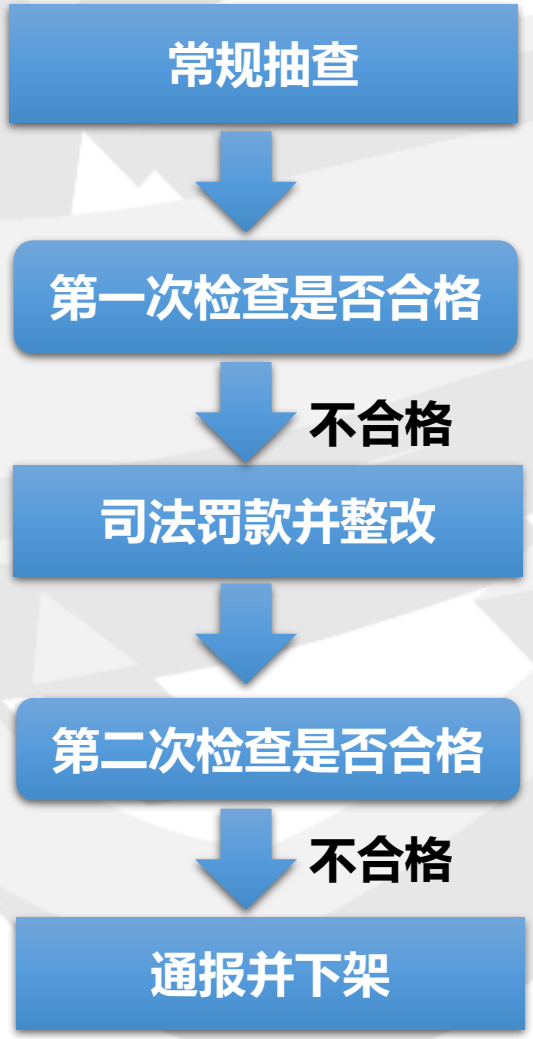
个人信息主体

个人信息所标识的自然人。

[GB/T 35273-2017，定义 3.3]

公安部网络安全保卫局、北京网络行业协会、公安部第三研究所联合发布《互联网个人信息安全保护指南》

公安部个人信息安全检查流程



近期合规性事件

工信部谈个人信息保护：拒不接受整治的APP要坚决下架

日期：2021-03-01 16:09 来源：中国新闻网

工信部部长肖亚庆介绍，去年来工信部对APP开展了专项整治，也和其他部门一起，对群众反映强烈的问题进行专项整治。今年还要继续延续整治，把大家反映的重点领域，按照最小可用的原则来处理个人信息使用问题。“在个人信息保护过程中，对这些拒不接受整治的APP要坚决下架。”

国新办今日就工业和信息化发展情况举行发布会，有记者提问，工信部认为中国科技公司在保护数据隐私方面做得如何？工信部在加强数据隐私和保护方面会采取哪些措施？比如中国将如何确保应用程序不再与第三方共享个人信息？

“个人信息保护问题，中国政府历来高度重视，我觉得就2020年来讲，在历史上可能是保护得最好的一年，因为我们是不断进步的过程。”肖亚庆首先指出。

肖亚庆介绍，监管在发展过程中，对个人信息应用的技术还有不少需要迅速提高、迅速加强的地方。手机APP的数量是非常大的，据不完全统计，有的说超过了350万，有的说保守估计也有250万以上。怎么样把这个监管好，工信部这些年也根据发展和安全要求加大了整治力度。

去年来工信部对APP开展了专项整治，也和其他部门一起，对群众反映强烈的问题进行了专项整治。比如说大家反映手机上的麦克风、手机里的通信地址等进行了专项整治。整治总体来讲，效果还是明显的。

“随着今年要求进一步提升，我们还要继续延续这样的整治，把大家反映的重点领域，按照最小可用的原则来处理个人信息使用问题。”肖亚庆表示。

“在个人信息保护过程中，对这些拒不接受整治的APP要坚决下架。”肖亚庆表示，同时，作为监管方面，也要提高技术装备能力，首先要能检测出这些信息保护的漏洞，使群众在这方面放心使用。

肖亚庆举例说，在APP中大家不喜欢的广告里面，找那个“×”非常难找。“所以信息骚扰可以拦截，如果不乐意看这个广告，应该非常明显可以关掉。”

肖亚庆表示，中国政府保护个人信息的态度是坚决的，法律是不断完善的，技术水平也在不断提升，我们要把行动坚持下去，一定会让大家不断有获得感。“我也公布一个电话，12321网络不良和垃圾信息举报受理中心平台，如果有什么问题，大家可以举报，这也是对我们工作的促进。”肖亚庆最后表示。

近期合规性事件

关于侵害用户权益行为的APP通报（2021年第3批，总第12批）

2021-03-13 15:37　来源：　工业和信息化部网站　【字体：大 中 小】　打印

依据《网络安全法》《电信条例》《电信和互联网用户个人信息保护规定》等法律法规，按照《关于开展纵深推进APP侵害用户权益专项整治行动的通知》（工信部信管函〔2020〕164号）工作部署，我部近期组织第三方检测机构对手机应用软件进行检查，督促存在问题的企业进行整改。截至目前，尚有136款APP未完成整改（详见附件），上述APP应在3月17日前完成整改落实工作。逾期不整改的，我部将依法依规组织开展相关处置工作。

附件：存在问题的应用软件名单（2021年第3批，总第12批）

工业和信息化部信息通信管理局

2021年3月11日

序号	应用名称	应用开发者	应用来源	版本号	所涉问题
1	腾讯手机管家	深圳市腾讯计算机系统有限公司	豌豆荚	8.10.2	APP频繁自启动和关联启动
2	诸葛天气	上海懿瞳信息科技有限公司	vivo应用商店	3.13	应用分发平台上的APP信息明示不到位
3	2345天气王	上海二三四五网络科技有限公司	小米应用商店	9.5.3	超范围收集个人信息
					APP强制、频繁、过度索取权限
4	荔枝新闻	江苏长江传媒有限责任公司	vivo应用商店	7.22	超范围收集个人信息
					违规使用个人信息

2020.5.16 公安部

《违法违规收集个人信息192个APP被责令改正》

今年第一季度，全国公安机关网安部门加大公民个人信息保护力度，依法查处违法违规收集公民个人信息APP服务单位386个，涉及信息咨询、辅助学习、文学小说、新闻资讯、娱乐播报等多个类型。其中，97个APP被予以行政处罚，192个APP被依法责令改正违法行为，51个APP被下架、停运，公民个人信息得到有效保护。今天，警方发布违法收集公民个人信息十大案例：

“猎豹清理大师”APP（版本号：6.13.5.1066）。经查，该款APP的隐私协议中对于索取用户通讯录、通话记录等权限的行为没有进行详细说明。北京市公安局朝阳分局已依法责令该公司改正违法行为。

“印象笔记”APP（版本号：10.5.5）。经查，该款APP隐私协议中未以显著位置、显著字体申明收集用户信息数据项，未明示各数据项收集用途。北京市公安局朝阳分局已依法责令该公司改正违法行为，并予以警告处罚。

“好孕帮”APP(版本号：3.4.8)。经查，该款APP在收集信息时未明示并征得用户同意，用户服务协议及隐私声明中未明示申请权限目的，未告知收集用户个人信息的目的及使用方式。北京市公安局西城分局已依法责令该公司改正违法行为，并予以警告处罚。

“不背单词”APP(版本号：3.2.2)。经查，该款APP在收集信息时未明示取得用户同意。北京市公安局大兴分局已依法责令该公司改正违法行为，并予以警告处罚。

“哈弗智家”APP(版本号：3.4.7)。经查，该款APP无收集信息明示且未取得用户同意，未向用户明示收集、使用个人信息的目的、方式、范围。河北省保定市公安局已依法责令该公司改正违法行为。

近期合规性事件

2021.5.1网信办

《违法违规收集使用个人信息33款APP被责令改正》

关于输入法等33款App违法违规收集使用个人信息情况的通报

2021年05月01日 09:00　　来源：中国网信网　　【打印】【纠错】

关于输入法等33款App违法违规收集使用个人信息情况的通报

近期，针对人民群众反映强烈的App非法获取、超范围收集、过度索权等侵害个人信息的现象，国家互联网信息办公室依据《中华人民共和国网络安全法》《App违法违规收集使用个人信息行为认定方法》等法律和有关规定，组织对输入法、地图导航等常见类型公众大量使用的部分App的个人信息收集使用情况进行了检测。现将有关情况通报如下：

一、输入法类App情况

序号	App 名称	版本	运营者	存在的主要问题
1	搜狗输入法	10.24.1	北京搜狗信息服务有限公司	违反必要原则，收集与其提供的服务无关的个人信息等。
2	讯飞输入法	10.0.11	科大讯飞股份有限公司	违反必要原则，收集与其提供的服务无关的个人信息等。
3	百度输入法	10.1.2.5	百度在线网络技术（北京）有限公司	违反必要原则，收集与其提供的服务无关的个人信息等。
4	章鱼输入法	5.1.7	北京智慧章鱼科技有限公司	违反必要原则，收集与其提供的服务无关的个人信息等。

近期合规性事件

工业和信息化部严厉查处“3·15”晚会曝光“诱导老年人下载APP”“APP违规收集老年人个人信息”等违规行为

发布时间：2021-03-16 14:03　来源：信息通信管理局

关于侵害用户权益行为的APP通报（2021年第1批 总第10批）

发布时间：2021-01-22 19:45　来源：信息通信管理局

江西通信管理局深入开展APP侵害用户权益专项整治

发布时间：2020-12-16 14:33　来源：江西省通信管理局

国家网信办通报腾讯手机管家等84款App违法违规收集使用个人信息情况

界面新闻
发布时间: 05-10 12:04 | 界面新闻官方帐号,优质财经领域创作者

国家计算机病毒应急处理中心监测发现多款违法移动应用

新华社
发布时间: 20-12-04 18:36 | 新华社官方帐号

国家计算机病毒应急处理中心监测发现十四款违法移动应用

新华网客户端
发布时间: 20-09-11 11:36 | 新华网官方帐号

公安部：查处违法违规收集公民个人信息APP服务单位386个

封面新闻
发布时间: 20-05-18 12:53 | 封面新闻官方帐号

国家网信办通报Keep、今日头条等129款App违法违规收集使用个人信息情况

人民网
发布时间: 06-11 16:17 | 人民网官方帐号

企业痛点

问题修复

难以全面审查自身及

第三方SDK合规性

成本

产品 / 技术 / 法务

投入费用高

红线把控

国家监管政策掌握不到位

缺乏相应政策专家

技术

难以全面审查自身及

第三方SDK合规性

违规APP首次修改后合规率 **低于 30%**

海云安
secidea

PART02

解决方案

解决方案

引擎+平台

APP行为分析引擎

自动专业APP行为分析、网络分析、逆向分析等领先技术，实现对APP实时正式行为分析，全面识别隐藏个人信息收集、传输、使用等行为

个人信息核查平台

通过web平台化进行测试过程录入，提供详细测试用例和测试方法说明，便捷录入，自动生成报告

检测方式

1、采取技术+管理相结合，人工+工具相融合的方式，深挖问题隐患，全面洞悉风险；

2、有效结合现有APP安全检测工作，快速掌握移动应用中个人信息安全状况，开展持续检测。

检测内容

个人信息安全检测

违规收集用户个人信息

- 私自收集个人信息
- 超范围收集个人信息

违规使用用户个人信息

- 私自共享给第三方
- 强制用户使用定向推送功能

不合理索取用户权限

- 不给权限不让用
- 频繁申请权限
- 过度索取权限

为用户账号注销设置障碍

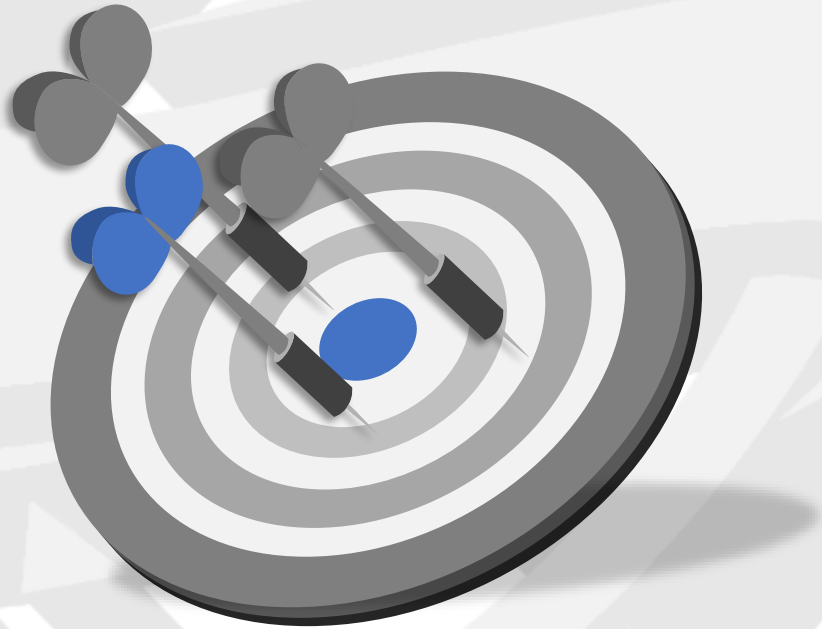
- 账号注销难

应用安全检测

核心技术

专项行为监测技术

运用目前HOOK技术，通过定制HOOK系统环境实现对应用组件调用信息等行为监测和行为分析，极大提高对移动应用的逆向破解、敏感行为分析、违法违规行为分析能力。



检测对抗技术

采用自动化检测技术对抗方法，基于动态分析和防护特征，可以统一绕过APP安全保护功能，提高自动化分析能力。

插件架构实现技术

插件框架以插件的形式组织、管理具体分析中的功能组件，由插件接口规范、配置管理、服务发布管理、部署等，通过插件接口各类插件接入和加载运行

标准依据

1、TC260-PG-20202A APP收集使用个人信息自评估指南

2、国信办秘字[2019]191号《App违法违规收集使用个人信息行为认定方法》

3、GB/T 35273-2020《信息安全技术 个人信息安全规范》

4、GA 1277 信息安全技术 互联网交互式服务安全保护要求

5、GB/T 20984 信息1安全技术 信息安全风险评估规范

6、《中华人民共和国网络安全法》

7、信息安全相关监管要求《移动互联网应用程序信息服务管理规定》

8、工信部信管函〔2019〕337号《工业和信息化部关于开展APP侵害用户权益专项整治工作的通知》

9、工信部信管函〔2020〕164号《工业和信息化部关于开展纵深推进APP侵害用户权益专项整治行动的通知》

10、国信办秘字〔2021〕14号四部门联合发布《常见类型移动互联网应用程序必要个人信息范围规定》

深度发现敏感行为

所有 | 个人信息分析 | 文件访问信息 | 网络传输信息 | 组件调用 | 其他敏感行为 | 加解密及证书

全选 申请高危权限 申请高危权限2 获取设备id 获取imei码 获取系统版本 获取手机号 获取位置信息 获取位置信息2 读取手机重要数据（uri） 读取手机imsi 读取手机串号 读取SIM卡提供商代码
读取ISO标准的国家 读取网络状态 读取MCC+MNC代码 读取移动网络运营商的名字(SPN) 读取wifi 读取剪切板 读取剪切板2 读取取地理位置 读取手机应用列表 读取默认浏览器Cookie 录音 录音/录像
读取拍照图片 获取运营商名称 获取mac 获取wifi广播 获取ip 获取ip2 获取网络国家编号 获取调试状态 获取安装包名 获取安装应用 获取安装模块 获取安装包名2 发送短信 发送短信2
获取定位 录音 获取手机应用列表

读取手机重要数据（uri） 14:58:21.1 J [Hook android.content.ContentResolver.query success, after hook, parameter(s): param1(android.net.Uri$StringUri): content://sms/, param2([Ljava.lang.String;): _id, address, person, body, date, type,,, param5(java.lang.String): date desc, return(android.content.ContentResolver$CursorWrapperInner): android.content.ContentResolver$CursorWrapperInner@28ae6cd1]

读取手机重要数据（uri） 14:58:21.1 J [Hook andro
type,,, param5(java.lang.String): date desc,, return(android.co

读取手机重要数据（uri） 14:58:21.9 J [Hook andro
date, type,,, param5(java.lang.String): date desc,]

读取手机重要数据（uri） 14:58:21.9 J [Hook andro
date, type,,, param5(java.lang.String): date desc]

读取网络状态 14:58:21.1 J [Hook android.telephon

获取设备id 14:58:20.995 J [Hook android.telephony.

获取手机应用列表 14:57:30.912 J [Hook android.app.
com.google.android.youtube}, PackageInfo{3d502670 com.a
com.android.providers.calendar}, PackageInfo{3269399c com
com.android.wallpapercropper}, PackageInfo{49e5388 com.a
com.google.android.apps.enterprise.dmagent}, PackageInfo{
com.android.phasebeamorange}, PackageInfo{24b20ba0 con
com.android.providers.downloads.ui}, PackageInfo{1fbc41cc

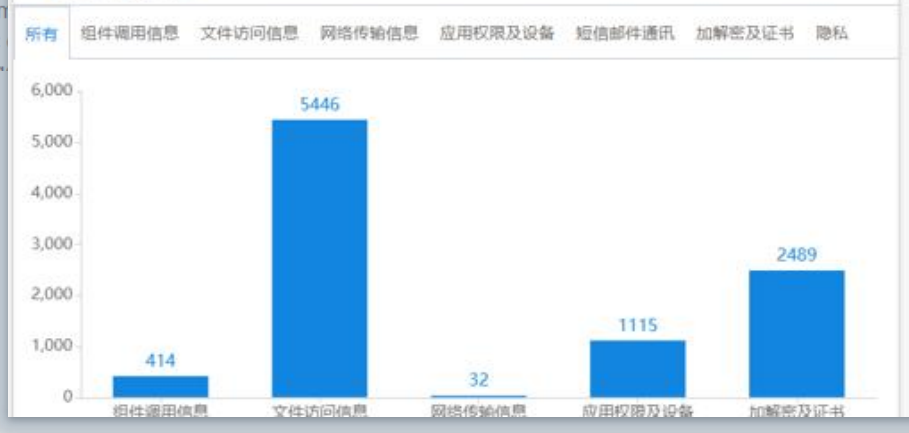
行为分析统计

包名：
加固情况：加固 (未识别高级加固)
MD5：77a04c44d7a8af1b327ab227ebb3b970
创建时间：2020-04-20 15:18:01
结束时间：2020-04-20 15:22:01
版本号：2.4.178
文件大小：16648KB

APK下载 脱壳包下载 分析详情

各类接口占比

接口调用分布



接口调用历史

海云安
secidea

PART03

服务内容

个人信息安全检测服务

标准解读

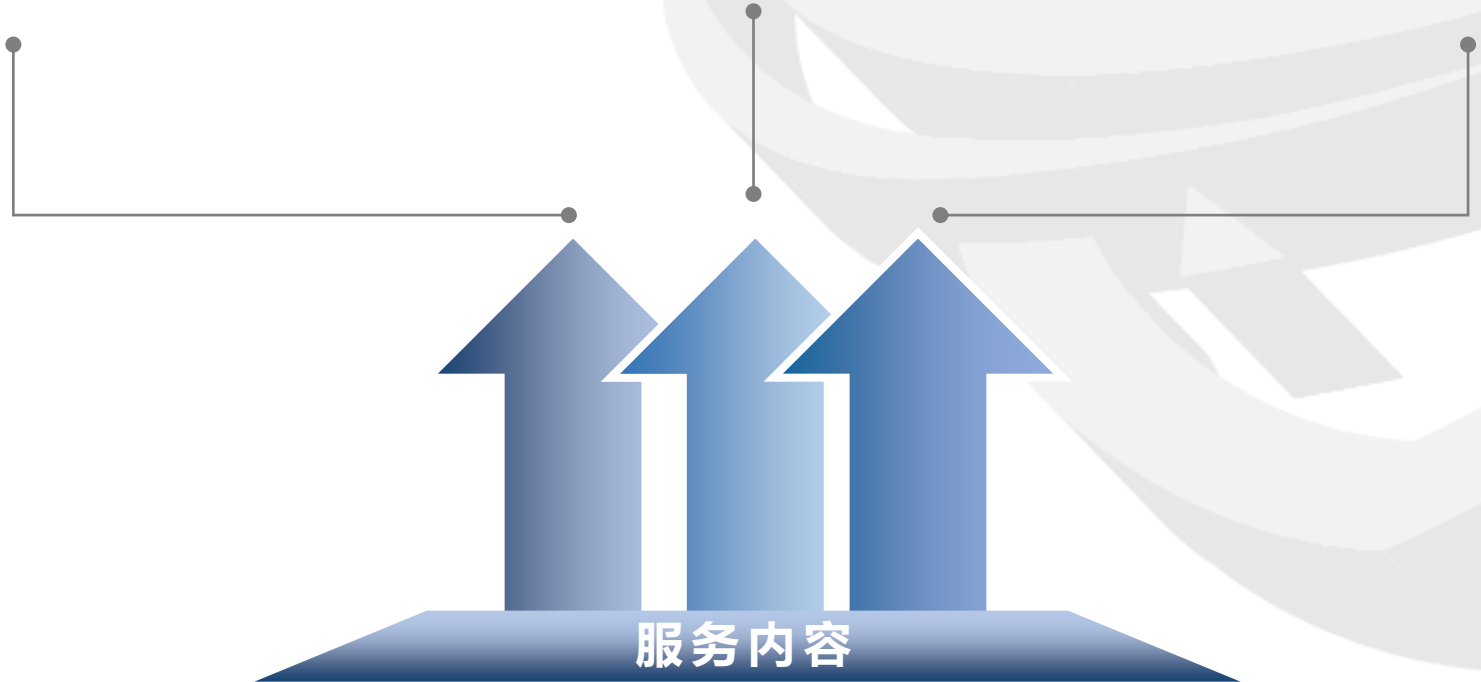
为APP客户提供的咨询和测试服务，所参考的标准是App专项治理工作组自2019年以来，发布的一系列技术规范和标准文本。

产品评估

完全按照工信部等标准，提供最权威的政策和标准解读，输出APP评估报告，为企业给出可执行的具体整改意见。帮助企业未雨绸缪，避免相关问题。

协助沟通

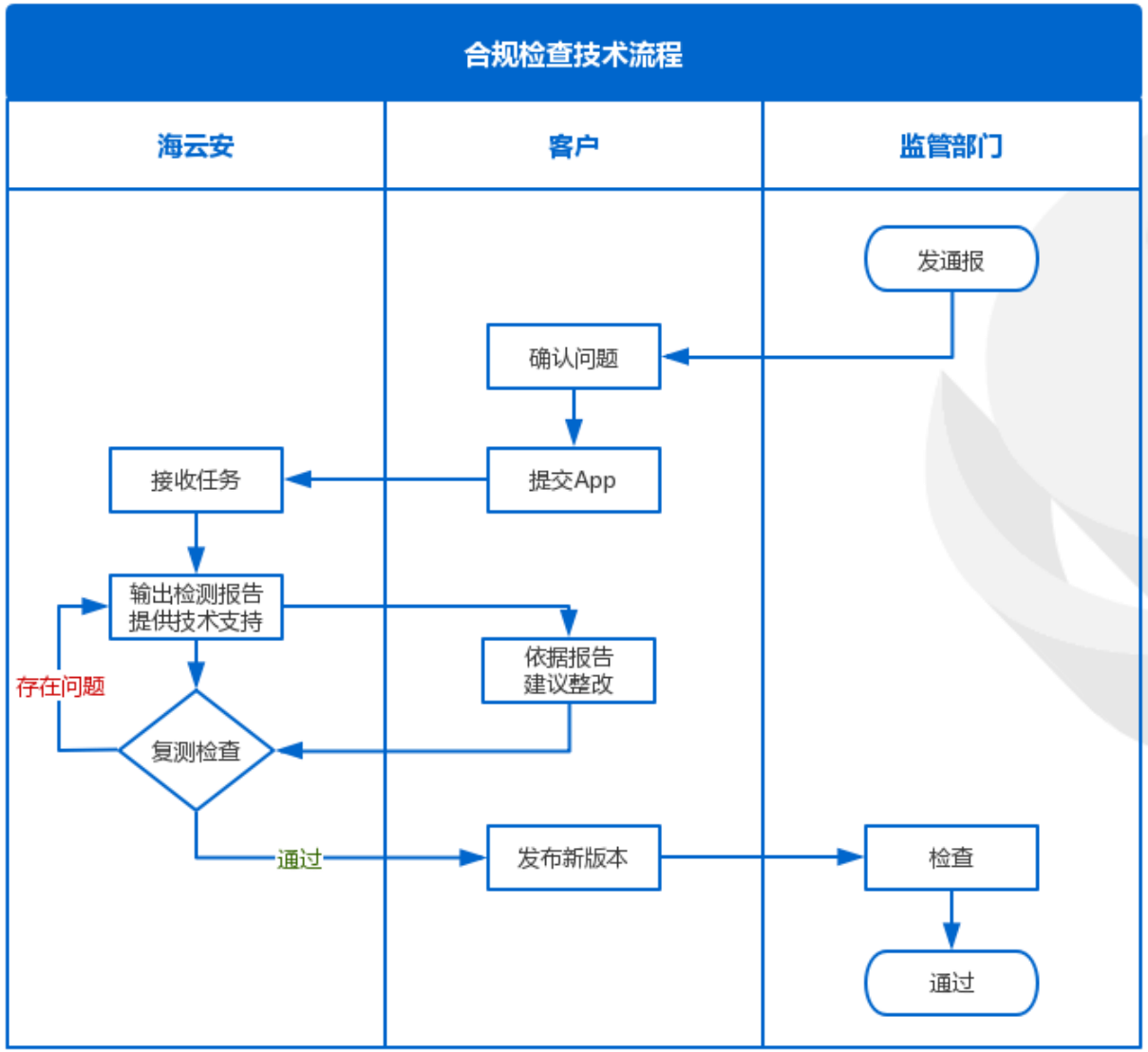
App产品有其独特性，我方基于对App产品的深入理解，帮助企业与政府监管部门有效沟通，在保证产品合规的前提下，不降低产品的服务质量。



服务内容

服务名称	服务类型	服务内容	服务期限
服务项目	合规检测服务	服务期内，指定APP两个不同版本的初检、复检服务（含检测报告及整改意见）	6次/年
	整改服务	输出整改建议报告，并提供相应的整改咨询服务	6次/年
	政策咨询服务	服务期内不限次数法律及政策咨询	1年
		相关标准解读、最新政策解读、7x24小时专人服务	1年

服务流程



签署合同

一周内

提交需测试版本APP

两周内

出具测试报告及整改建议

Thanks

海云安 secidea

可信应用
主动防御