人脸识别技术在 App 应用中的隐私安全研究报告

（2020 年）

中国信息通信研究院安全研究所
北京百度网讯科技有限公司

2020 年 6 月

版权声明

本报告版权属于中国信息通信研究院安全研究所、北京百度网讯科技有限公司，并受法律保护。转载、摘编或利用其它方式使用本蓝皮书文字或者观点的，应注明“来源：中国信息通信研究院安全研究所、北京百度网讯科技有限公司”。违反上述声明者，本院将追究其相关法律责任。

编 写 团 队

编写单位：

中国信息通信研究院安全研究所

北京百度网讯科技有限公司

编写组成员：（姓氏笔画为序）

王然、王磊、王洋、王海棠、刘焱、陈湉、杜悦艺、吴月升、唐佳伟

CAICT 中国信通院

前　言

近两年，随着人脸识别技术的迅速发展，“刷脸”逐渐成为新时期生物识别技术应用的主要领域。尤其是在进入 2017 年之后，人脸识别更是迎来了井喷式的爆发，互联网企业面对法律法规以及某些业务上的需求，纷纷推出账号实名认证，并将人脸认证环节在相关 App 中实现。然而，人脸识别技术在快速发展、深入社会的同时，也给我们带来了诸多安全挑战。个人隐私数据泄漏、技术滥用等造成的信息安全风险问题亟待解决。

CAICT 中国信通院

目 录

一、人脸识别技术的基本情况.....1
(一) 人脸识别技术.....1
(二) 身份验证中的人脸识别技术应用示例.....2
(三) 人脸识别技术的特点.....3
(四) 人脸识别技术的难点.....4
二、人脸识别技术的应用.....5
(一) 人脸识别技术应用的市场前景.....5
(二) 企业研究人脸识别技术的应用概况.....7
(三) 人脸识别技术在 App 中的应用场景.....8
三、人脸识别 App 面临的安全风险.....14
(一) 网络和数据安全保障机制欠缺易造成人脸数据泄漏.....14
(二) 人脸识别技术应用不规范为人脸数据滥用提供可能.....15
(三) 人脸的深度伪造技术严重威胁用户财产甚至人身安全.....16
四、 人脸识别 App 的个人信息保护相关建议.....17
(一) 加快人脸识别相关法律法规研制进程.....17
(二) 加快构建人脸识别技术应用监管体系.....18
(三) 加快推进人脸识别技术的安全系列标准研制.....18
(四) 鼓励行业协会或社会组织开展行业自律.....19

CAICT 中国信通院

图 目 录

图 1　人脸识别在 App 中的身份验证流程图.....3
图 2　人脸识别市场应用分布图.....6
图 3　人脸识别行业产业链结构示意图.....7
图 4　10 款 App 的隐私行为统计图.....22

CAICT 中国信通院

表 目 录

表 1　2020 年我国计算机视觉市场规模预测 6

CAICT 中国信通院

一、 人脸识别技术的基本情况

人脸识别是基于人的脸部特征信息进行身份识别的一种生物识别技术。具体而言，就是计算机通过视频采集设备获取识别对象的面部图像，再利用核心的算法对其脸部的五官位置、脸型和角度等特征信息进行计算分析，进而和自身数据库里已有的范本进行比对，最后判断出用户的真实身份。

（一）人脸识别技术

从采集人脸到辨识人脸的整个流程上来看，人脸识别技术一般包括：人脸图像采集及检测、人脸特征提取（关键点提取）、人脸规整（图像处理）和人脸识别比对等。

1. 人脸图像采集及检测

不同的人脸图像都能通过摄像镜头采集下来，比如静态图像、动态图像、不同的位置、不同表情等方面都可以得到很好的采集。当用户在采集设备的拍摄范围内时，采集设备会自动搜索并拍摄用户的人脸图像。人脸检测在实际中主要用于人脸识别的预处理，即在图像中准确标定出人脸的位置和大小。

2. 人脸特征提取（关键点提取）

人脸识别系统可使用的特征通常分为视觉特征、像素统计特征、人脸图像变换系数特征、人脸图像代数特征等。人脸特征提取就是针对人脸的某些特征进行的。人脸特征提取，也称人脸表征，它是

对人脸进行特征建模的过程。人脸特征提取的方法归纳起来分为两大类：一种是基于知识的表征方法；另外一种是基于代数特征或统计学习的表征方法。

3. 人脸规整（图像处理）

对于人脸的图像预处理是基于人脸检测结果，对图像进行处理并最终服务于特征提取的过程。系统获取的原始图像由于受到各种条件的限制和随机干扰，往往不能直接使用，必须在图像处理的早期阶段对它进行灰度校正、噪声过滤等图像预处理。对于人脸图像而言，其预处理过程主要包括人脸图像的光线补偿、灰度变换、直方图均衡化、归一化、几何校正、滤波以及锐化等。

4. 人脸识别对比

提取的人脸图像的特征数据与数据库中存储的特征模板进行搜索匹配，通过设定一个阈值，当相似度超过这一阈值，则把匹配得到的结果输出。人脸识别就是将待识别的人脸特征与已得到的人脸特征模板进行比较，根据相似程度对人脸的身份信息进行判断。可分为 1:1、1:N、属性识别。其中 1:1 是将 2 张人脸对应的特征值向量进行比对,1:N 是将 1 张人脸照片的特征值向量和另外 N 张人脸对应的特征值向量进行比对，输出相似度最高或者相似度排名前 X 的人脸。

（二）身份验证中的人脸识别技术应用示例

目前很多 App 加入了人脸识别功能，然而现在人脸识别应用还处于初级阶段，目前我国应用最多还是 1：1 等级，也就是人脸识别中最初级的“证明你是你”，一般应用于身份核对方面。具体的人脸识别在 App 中的身份验证流程如图 1 所示。



数据来源：CSDN 博客

图 1　人脸识别在 App 中的身份验证流程图

用户拍摄自己身份证信息并上传 App，App 经过公民身份信息查询获取用户信息及身份证系统证件照片，建立用户档案并关联用户人脸；当 App 扫描用户人像时，经活体检测、人脸质量检测、人脸图像等处理后与先前获取的用户人像照片进行人脸对比，完成身份验证的过程。

（三）人脸识别技术的特点

人脸识别的优势在于其自然性和不被被测个体察觉的特点。

1. 自然性

自然性是指该识别方式同人类（甚至其他生物）进行个体识别时所利用的生物特征相同。例如人脸识别，人类也是通过观察比较人脸区分和确认身份的，另外具有自然性的识别还有语音识别、体

形识别等，而指纹识别、虹膜识别等都不具有自然性，因为人类或者其他生物并不通过此类生物特征区别个体。

2. 非接触性

人脸识别完全利用可见光获取人脸图像信息，不同于指纹识别需要利用手指接触传感器采集指纹，用户不需人脸与设备直接来接触，可以同时满足多人连续进行人脸图像信息的识别和分拣，在医院测温、小区门禁等一些应用场景下人脸识别技术的非接触性特点可为用户提供便利。

（四）人脸识别技术的难点

人脸识别被认为是生物特征识别领域甚至人工智能领域最困难的研究课题之一。人脸识别的困难主要是人脸作为生物特征的特点所带来的。

1. 相似性

不同个体之间的区别不大，所有的人脸的结构都相似，甚至人脸器官的结构外形都很相似。这样的特点对于利用人脸进行定位是有利的，但是对于利用人脸区分人类个体是不利的。例如双胞胎现象，全世界双胞胎平均出生率为 1：89，有些双胞胎面部存在差异，有些双胞胎甚至从面部特征来看相似度极高，对于人脸识别系统形成非常大的挑战，几乎从生物特征上很难区别出个体。

2. 易变性

人脸的面部特征具有不稳定性，人可以通过脸部的变化产生很多表情，而在不同观察角度，人脸的视觉图像也相差很大。另外，人脸识别还受光照条件（例如白天和夜晚，室内和室外等）、人脸的很多遮盖物（例如口罩、墨镜、头发、胡须等）、年龄等多方面因素的影响。

3. 易攻击性

随着数字拍照、视频合成技术等发展，越来越容易获得某个特定人的人脸信息或者合成人脸信息。更甚至随着对抗训练（Adversarial Training）的深度学习技术的发展，计算机可以合成高精度的任何人的人脸信息。

二、人脸识别技术的应用

近年来，由于人工智能的飞速发展，人脸识别技术取得了显著的发展，被广泛使用于身份认证等实际应用中，小到日常的手机屏幕人脸解锁，大到政府部门使用人脸识别技术进行公民的身份认定，人脸识别技术已经逐渐普及到人们的日常生活中。

（一）人脸识别技术应用的市场前景

2018 年中国计算机视觉人脸识别市场规模为 151.7 亿元。根据前瞻产业研究院对六大权威机构的汇总，乐观估计 2020 年我国计算机视觉市场规模有望突破 1000 亿，具体数据如表一所示；中性预测 2020 年我国计算机视觉市场规模在 700 亿元左右，市场发展前景可

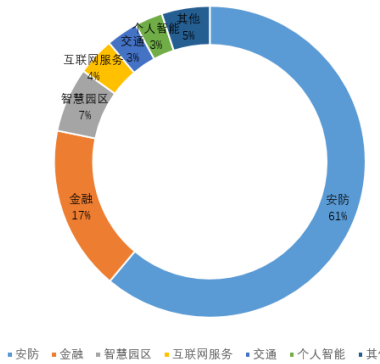
期。

表一 2020 年我国计算机视觉市场规模预测

机构类型	机构	规模	复合增长率
国内机构	CAICT	600 亿元	96%
	腾讯研究院	660 亿元	110%左右
	艾瑞咨询	725 亿元	162.7%
	艾媒 iiMedia Research	780 亿元	125.5%
国外机构	Ganter	110 亿美元	117%
	CB Insight	160 亿美元	128%

数据来源：前瞻产业研究院

根据亿欧智库研究报告显示，人脸识别市场应用涵盖安防、金融、智慧园区、交通出行、互联网服务等多个行业领域。根据亿欧智库的统计结果显示，2018 年安防占人脸识别市场份额的 61.1%，金融占 17.1%，智慧园区占 6.7%，互联网服务占 3.9%，交通出行占 3.3%，个人智能占 2.9%，其他（包括：智能汽车、智能零售、政务服务、运营商服务等）占 5.0%，人脸识别应用市场份额分布如图 2 所示。



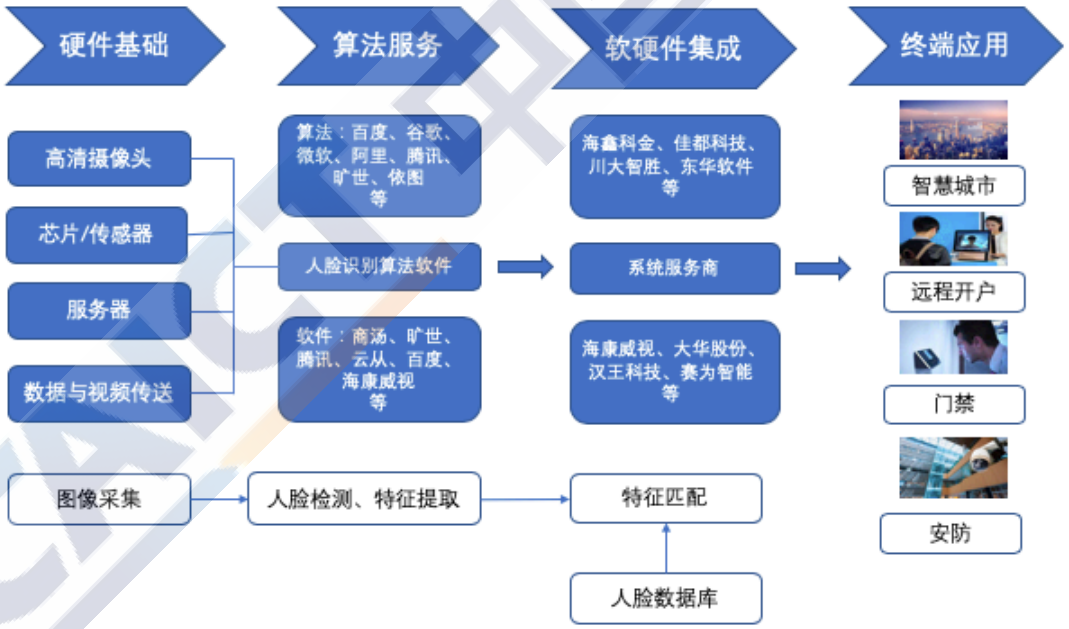
数据来源：亿欧智库研究报告

图 2 人脸识别市场应用分布图

从以上数据可以看出，人脸识别技术应用越来越广泛，为经济社会的发展以及人们日常生活的便捷带来了新机遇。

（二）企业研究人脸识别技术的应用概况

人脸识别目前在国内发展迅速，各种新兴企业如雨后春笋，中国人脸识别的独角兽：旷视科技，商汤科技。同时，云从科技，依图科技等初创公司也在持续发力抢夺市场。从人脸识别行业产业链条来看（如图 3 所示），人脸识别产业的上游是硬件基础的支撑，包括高清摄像头、处理芯片(CPU、GPU、TPU)、服务器和数据与视频传输设备；产业链中游主要是人脸识别算法和软件服务；产业链下游则是具体的场景应用，即应用方案、消费类终端或服务等。



数据来源：前瞻产业研究院整理

图 3　人脸识别行业产业链结构示意图

国内的互联网企业百度、阿里巴巴、腾讯对人脸识别这个方向相当重视，阿里巴巴控股旷视科技、商汤科技、依图科技，并且开

发了自己的人脸识别接口，已全面将人脸识别技术应用到支付宝、淘宝等 App 中，并联合集团旗下其他业务板块，研究人脸识别的应用场景；腾讯旗下拥有自己的优图团队，为 QQ 空间、腾讯地图、腾讯游戏等 50 多款 App 提供图像技术支持；百度人脸识别也依靠庞大的数据资源发展迅速，通过使用人脸识别技术已推出百度识图、脸优等 App。除此之外，这三家大型互联网企业可以为开发者提供开放平台并免费进行调试。

（三）人脸识别技术在 App 中的应用场景

随着人脸识别技术的日益成熟，我们可以看到已经有很多 App 用到了人脸识别技术，特别是金融和互联网领域的 App 纷纷接入了人脸识别技术应用于身份识别和面部特征提取分析。目前，人脸识别技术主要应用在金融类、在线教育类、电信类、出行类、美图娱乐类、电商类、智慧园区类 App 中。本报告将分析人脸识别技术在这 7 类 App 中具体的应用场景以及应用的目的和存在的问题。

1. 金融类 App 中的应用场景

金融类 App 接入人脸识别功能最主要是为了保障用户在使用过程中的资金交易安全性。以互联网金融行业中最具代表性的 “支付宝”这一款 App 为例进行说明，用户在利用“借呗”借钱时，除了输入密码之外一般还需要进行人脸检测来确认此时的 App 操作者是本人，通过人脸识别可以有效防止支付宝账号被盗造成用户财产损失的情况发生。除此之外，金融类 App 还可以通过人脸识别技术提

供远程开户、绑卡核身、账户登录、分期购物、人脸考勤、人脸支付等服务。

在人脸识别落地金融行业过程中，各大银行也纷纷尝试将人脸识别引入刷脸支付、即时开卡、VTM 等金融场景中，但从技术角度来看，人脸识别并不是万能的。虽然现在人脸识别技术已经非常成熟，但是光线条件、天气（雨、雪、雾）、用户整容等仍然会影响人脸识别结果。人脸识别在转账支付、即时开卡等高安全级别业务中的应用还是需要更审慎一些，不能单纯依靠人脸识别技术来解决用户身份核查的问题，还需要采用包括人脸识别在内的双因素甚至多因素认证来提升身份核查在金融领域的安全性。

2. 在线教育类 App 的应用场景

在线教育类 App 接入人脸识别功能的用途之一是为了查验学员身份，避免一账号多个人使用的情况，给网校造成损失。通过人脸识别可以很大程度降低账号共用的问题，通过一定频率的触发人脸识别机制，校验当前使用网校账号的面孔是否为存储在系统中的面部图像，若系统识别为同一学员，则继续进行当前的操作，若识别到是不同的人，则会强制退出登录。除此之外，人脸识别功能的另一用途是帮助在线课堂老师了解学生学习状态。在线课程与线下课堂不同，可能同时有数千名学生在远程听课，老师无法通过观察每位学生的表情来识别学生对于课程的接收程度。通过面部表情识别可以让教师更加理解学生的需求，弥补网络授课相较于传统授课在

师生交流环节上的不足。

在线教育类 App 主要服务对象是中小学生，其中大多数是未满 14 周岁的儿童，由于儿童认知能力、危险识别能力和自我保护能力相对薄弱，儿童的个人生物识别信息更是社会各界保护的重点。2019 年 9 月 5 日，教育部科学技术司司长雷朝滋在教育部新闻发布会上针对在线教育 App 采集学生的个人信息安全问题表示，“能不采就不采，能够少采就少采，尤其是涉及到学生个人生物信息，对于人脸识别或者肢体识别的教育 APP 加以限制和规范，同时我们希望学校慎重使用。”除此之外，根据南都个人信息保护研究中心发布的《人脸识别落地场景观察报告（2019）》的调研结果显示，33.84%的受访人员不同意将人脸识别技术应用到教育类相关系统中。由此可见，在对未成年人使用人脸识别技术时应更加谨慎，通过安全保障措施加强对未成年人的权益保护。

3. 电信类 App 的应用场景

电信类 App 接入人脸识别功能的主要目的是为了实现 SIM 卡激活过程中的实人认证。以“中国移动 App”为例，用户在中国移动 App 上购买 SIM 卡之后，需要在 App 的“卡号激活”业务功能中完成实人认证，在激活的过程中上传身份证信息后进行人像视频认证，视频认证过程中需要用户录制一段 6 秒的视屏，录制的内容为朗读屏幕上随机产生的 4 位验证码。视频审核通过后 SIM 卡才可激活成功。

2019 年 9 月 27 日，工信部办公厅印发了《关于进一步做好电话用户实名登记管理有关工作的通知》，指导电信企业扎实开展电话用户实名登记工作。为确保电话入网环节人证一致，创新运用人工智能等技术手段，工信部要求电信企业自 2019 年 12 月 1 日起在实体渠道全面实施人像比对技术措施，人像比对一致后方可办理入网手续。因此，为了维护公民在网络空间的合法权益，有效防范电信网络诈骗的问题，在线上办理SIM卡激活时也同样需要进行人脸识别。

4. 出行类 App 的应用场景

出行类App接入人脸识别功能能够最大限度的保障司机的安全、乘客的安全以及载运货物的安全。以“滴滴出行”这一款人脸识别 App 为例进行说明，司机在 App 中填写完各种基础资料之后，还需要进行人脸图像的认证这最后一步操作才能进行接单，它一方面可以保障司机的身份信息和财产安全，防止出现盗号的情况；另一方面也可以保障乘客的人身安全，防止遇到不良司机。

2018 年 9 月 11 日，交通运输部、中央网信办、公安部等多部门组成的专项工作检查组陆续进驻网约车和顺风车平台公司，开展安全专项检查，并且规定相关 App 在派单前应用人脸识别等技术，对车辆和驾驶员一致性进行审查。同时，人脸识别技术应用到出行类 App 中可以有效保障司机、乘客的财产和人身安全。

5. 美图娱乐类 App 的应用场景

美图娱乐类 App 接入人脸识别功能除了保障账号安全性之外还

可以利用人脸识别功能实现各种极具创意的互动营销活动。以“美图秀秀”这一款人脸识别 App 为例进行说明，用户在下载美图秀秀软件进行拍照后，一般都会使用图片美颜功能，此时 App 可接入人脸关键点定位功能来帮助用户定位包括眉毛、眼睛、下巴等在内的人脸关键部位，方便用户使用美颜功能。同时，用户还可以自定义设计个性夸张、搞怪、迥异的人脸照片。除此之外，美图娱乐类 App，例如去年十分火爆的 ZAO，还可通过人脸识别技术提供照片换脸、视频换脸、同款表情包、换装换发型等服务。

美图娱乐类 App 使用人脸识别技术是业务功能所必要的，但是应对其收集、使用个人生物识别信息进行规范。新版《信息安全技术 个人信息安全规范》（以下简称《规范》）规定，收集个人生物识别信息前应单独告知使用目的、方式和范围，并征得个人信息主体的明示同意。同时，《规范》还规定原则上不应存储原始个人生物识别信息。因此，在美图娱乐类 App 扩展业务功能中应该本着最小必要原则合理使用人脸识别技术，并应按照《规范》单独告知并征得用户同意，当用户拒绝授权扩展业务功能使用人脸识别技术的相关权限时，App 不得反复征求授权，也不能影响其他与该权限无关的业务功能的使用。

6. 电商类 App 的应用场景

电商类 App 接入人脸识别功能的主要用途之一是为了保障用户账号的安全。通常作法是在登录账号时进行人脸识别实现实人认证，

防止不法分子通过破解密码登录用户账号。其次，电商类 App 为了提升用户服务体验，利用人脸识别功能提供在线换装、试戴等服务。除此之外，电商类 App 的人脸识别应用场景还包括：后台图像数据管理，即对违禁图片和广告图片的管理、直播、短视频等。

电商类 App 使用人脸识别技术基本上都是为了提升用户服务体验、增强用户粘性或者为用户提供便捷性，属于电商类 App 的扩展业务功能。因此，电商类 App 在使用人脸识别技术获取面部特征信息时，应告知并征得用户的同意，用户有权拒绝使用相关服务，不可强制要求用户提供面部特征信息。

7. 智慧园区类 App 的应用场景

智慧园区类 App 接入人脸识别功能主要是为了进行门禁管理、考勤管理、会议管理等。在门禁管理应用场景下，员工通过 App 实现一张脸解决企业楼宇园区内所有权限管理问题。在考勤管理应用场景下，App 基于人脸识别技术，结合网络和 GPS 定位，可以杜绝代打卡现象，解决外勤人员考勤难的问题。在会议管理应用场景下，参会人员通过录入人脸进行会议注册，会议签到时 App 的人脸识别功能会录入来宾面部信息，并自动与后台信息进行比对，可以快速地识别出来宾的身份。

智慧园区类 App 使用人脸识别技术为企业节省人工成本，操作高效快捷且便于管理。但是，智慧园区类 App 在使用人脸识别技术的过程中存在一定的风险，通过深度伪造来欺骗人脸检测的安全事

件层出不穷。因此，国家机关、保密单位等重要部门不应单纯依靠人脸识别技术进行门禁管理。

三、 人脸识别 App 面临的安全风险

人脸识别技术应用在提升身份认证便捷度和效率的同时，也给个人隐私和数据保护带来了巨大的挑战。通过评估具有人脸识别功能的 App 以及梳理国内外人脸识别相关的安全事件，本报告归纳总结出以下三方面的安全问题，并针对这三方面的安全问题分别挑选了应用市场中下载量较多的应用人脸识别技术的 App 进行了评估，评估结果见报告附件。

（一） 网络和数据安全保障机制欠缺易造成人脸数据泄漏

当前关于人脸识别技术的安全技术标准和使用规范不够完善，对于人脸数据控制者的责任和义务，人脸数据主体的权利以及人脸数据在收集、存储、处理等各环节应采取的安全措施缺少相关规定。因此，人脸识别技术的大部分开发企业和应用服务提供商已采取的安全措施可能难以应对人脸识别技术面临的安全威胁，容易发生人脸数据泄露等安全事件。除此之外，网络安全生态环境持续恶化，系统的安全漏洞几乎不可避免，因此人脸数据库泄漏事件也屡见不鲜。更为可怕的是，由于生物识别信息是唯一的，是不可再生的，因此，一旦丢失或者泄露，则是永久泄露，将贻害无穷。

2019 年 2 月 15 日，深网视界公司（主营业务为人脸识别、AI

和安防）被曝发生大规模数据泄露，致使 256 万人的个人信息能够不受限制地被访问，其中包含身份证号码、身份证发行日期、性别、国家、住址、生日、照片和过去 24 小时内的位置，大约有 668 万条记录。

2020 年 2 月 27 日，美国人脸识别初创企业 Clearview AI 称其整个客户名单被盗。据悉，Clearview AI 具有超过 30 亿张人像照片，形成了庞大的生物特征信息数据库。虽然本次案件声称仅泄露了客户名单，但 Clearview AI 数据库中 30 多亿人脸数据信息的安全性令人担忧。Clearview AI 律师表示，公司的系统跟网络并没有受到破坏，目前已修复了相关漏洞，并保证类似事件不会再次发生。

（二）人脸识别技术应用不规范为人脸数据滥用提供可能

随着人脸识别技术越来越普遍的应用到人们的生活中，人脸特征也逐渐成为了人们的身份证件之一，但是人脸识别技术的应用存在一些不规范的问题。首先，大部分 App 在采集人脸数据时并未依据《规范》单独明确告知并征得用户同意，甚至未在隐私政策中说明使用人脸识别技术的目的、范围和方式，使得人脸数据被动收集、使用成为常态。其次，部分社交娱乐类 App、在线教育类 App 未按照相关法律法规要求收集、使用人脸数据，导致人脸识别技术滥用事件时有发生。

2019 年 6 月 6 日，微软公司疑似因未经用户授权使用公众人物

面部照片的原因删除了曾为全球最大的人脸识别数据库 MS Celeb。据悉，MS Celeb 数据库拥有超过 1000 万张图像以及将近 10 万人的面部信息。在微软删除该数据库前，IBM、松下电气、阿里巴巴、辉达、日立、商汤科技、旷视科技等多个商业组织都曾使用过 MS Celeb 数据库。

2019 年 10 月 20 日，伊利诺伊州的一起集体诉讼案指控脸书公司滥用面部识别数据，脸书的人脸识别功能在未经过用户同意的情况下被自动激活，系统会要求用户识别照片中标记的人是否是他们认识的朋友。此案涉及 700 万用户，总罚款金额最高可能达到 350 亿美元。法庭文件说：“脸书的面部识别技术违反了伊利诺伊州的生物特征信息隐私法（BIPA）。违反 BIPA 的规定实际上损害了用户的隐私，或会对他们的隐私构成实质性的威胁。”

（三）人脸的深度伪造技术严重威胁用户财产甚至人身安全

由于人脸识别技术具有非接触性、成本低、检测快、自动学习等特点，人脸识别已经成为身份识别中的重要手段。但是，与人脸识别技术共同发展的，还有借助机器学习系统、图像视频更改人脸的“深度伪造”技术。自 2017 年以来，深度伪造技术开始活跃在网络中，随着这一技术算法的日趋成熟，无论是人像还是声音、视频都可以被伪造或合成，并可达到几乎不能辨别真伪的程度，身份欺骗成功率高达 99.5%，甚至成为许多人脸识别系统的克星。鉴于此，借助深度伪造技术破解人脸识别等验证系统，非法盗刷他人支付账户、获取他人个人信息或从事其他冒名的违法活动已成为可能，严重威胁到公民

财产安全和人身安全，甚至会使国家安全和公共安全受到威胁，引发社会忧虑和信任危机。

2018 年 5 月，美国总统特朗普宣布中止全球气候变化协议，随后被比利时某政党利用“深度伪造”技术篡改，做出一个“特朗普宣告比利时政府也应退出”的假视频，引起比利时民众的公愤。

根据浙江省衢州市中级人民法院的判决书显示，从 2018 年 7 月份开始，被告人张富、余杭飞等 4 人以牟利为目的，使用其购买的公民个人身份信息注册支付宝账号，并使用软件将公民头像照片制作成公民 3D 头像，从而通过支付宝人脸识别认证。通过这种方式来获取支付宝提供的邀请注册新支付宝用户的相应红包奖励，共获利 4 万元，现已判刑。

四、 人脸识别 App 的个人信息保护相关建议

有效防范人脸识别技术可能带来的风险和挑战需要从完善相关法规政策、加强政府监管、制度标准规范、提高行业自律和提升个体素养等层面系统规避，充分调动各界力量，共同营造良好发展生态。

（一）加快人脸识别相关法律法规研制进程

目前，我国对于公民生物信息等个人信息保护的相关法律法规散见于民法总则、网络安全法、消费者权益保护法以及最高法、最高检、国务院颁布的相关司法解释和规定中，内容上也都仅是对个人信息收集、使用、存储、传输等进行了一些原则性规定。因此，

我国需尽快完善包括人脸识别在内的个人生物信息使用的法律法规，明确法律要保护的公民个人生物信息的范围、公民个人生物信息保护的义务主体，强化责任追究，保障个人生物信息的安全、规范使用，加大对侵害公民个人隐私行为，特别是对个人生物信息泄露、滥用的处罚力度。

（二）加快构建人脸识别技术应用监管体系

建立人脸识别技术应用必要性评估制度。企业或组织在采用人脸识别技术前，需要根据技术实现方式、业务场景、数据收集使用情况，开展技术应用必要性评估；同时，相关监管部门可以预先建立人脸识别技术应用“负面清单”或“白名单”，以“清单+评估”的监管方式强化事前监管。此外，健全完善人脸识别技术应用事中评估和事后问责制度。一方面督促使用人脸识别技术的企业或组织依据相关安全规范，配套人脸识别技术安全防控措施，定期开展安全评估；另一方面，对发生人脸数据泄露等安全事件的涉事企业或组织严肃问责，并在三到五年内不定期对涉事企业进行回访持续监督。

（三）加快推进人脸识别技术的安全系列标准研制

人脸识别技术逐渐走向成熟，应用人脸识别技术的 App 越来越多，人脸识别技术的各类安全标准，包括保护个人生物信息的相关标准应尽快出台。建议围绕人脸识别技术的自身安全性、在 App 应用中的个人生物识别信息保护等方面的问题，加快研制人脸识别技

术的安全技术要求和管理要求、个人生物信息保护要求、安全应用规范等一系列标准，指导行业依据标准规范人脸识别技术在 App 中的使用行为，提升人脸识别技术的自身安全保护水平，降低 App 应用人脸识别技术的安全风险，从而保障用户个人生物信息的安全性。

（四）鼓励行业协会或社会组织开展行业自律

当今，以人脸识别技术为代表的人工智能技术发展日新月异。但是，由于人脸识别技术较为复杂，存在保障人脸数据安全难的问题。因此，建立人脸识别技术企业联盟类组织，鼓励相关行业协会或社会组织主动发挥行业自律平台作用，推动各利益相关方共同制定收集使用人脸数据的行为准则，推广宣传相关最佳实践，带动提升个人生物信息保护整体水平，有利于人脸识别行业良性发展。除此之外，App 运营者应自觉规范人脸识别技术在 App 中的应用，定期进行自评估或第三方评估。在采集人脸数据前须告知用途和可能风险，以保障用户知情权与选择权。同时，当用户不想再继续授权使用其人脸数据时，App 运营者必须提供“退出”或“删除”渠道，以确保用户的删除权。

附件：

一、关于人脸数据泄露安全问题的检测

本报告针对人脸数据泄露安全问题共检测了 14 款 App，包括金融类 4 款、在线教育类 2 款、政府应用类 2 款、美图娱乐类 5 款、出行类 1 款，人脸数据泄露安全检测项包括数据传输安全检测、数据接口安全检测（权限控制）和安全验证绕过检测等。通过检测发现，共有 5 款 App 存在数据泄露安全风险。

2 款在线教育类 App 均存在安全问题，其中 1 款 App 存在敏感数据明文传输、证书校验不当的安全问题，使用模拟器安装 App 之后，可以进行抓包，添加收货地址等请求对用户的隐私信息进行明文传输，存在中间人攻击泄露用户隐私信息的风险；另一款 App 存在安全验证绕过的安全问题，App 忘记密码功能使用 4 位短信验证码进行重置，短信验证码无过期时间相关的设置，攻击者通过暴力破解的方式可以重置任意用户密码。

1 款美图娱乐类 App 存在证书校验不当的安全问题，在 App 颜值管家功能中，用户自定义上传人脸特征数据，由于 App 未正确验证证书，存在中间人攻击风险，攻击者利用漏洞有可能窃取传输的人脸特征数据。

1 款金融类 App 存在敏感数据明文传输、json 劫持、越权访问的安全问题。在检测过程中发现手机号、身份证号、银行卡号等敏感信息并没有加密传输，攻击者可利用中间人劫持等手段获取明文

的敏感信息；在 App 个人中心功能界面时抓包到接口返回的明文邮箱地址，并且可添加 callback 参数，使响应包中返回 jsonp 格式数据。如果用户登录状态下点击攻击者给定的 url，攻击者可通过 script 标签跨域获取同花顺返回的个人信息，可造成明文邮箱、打码手机号等信息泄露；App 问答处可遍历所有用户提问，同时可越权查询用户股票开户进度，存在泄漏用户隐私信息的风险。

1 款政府应用类 App 存在安全验证绕过的安全问题。在登录和查询电子卡证时均可绕过人脸识别验证，虽然提示账号身份已过期请重新登录，但是依然可以获取公积金信息。

二、关于数据违法违规使用安全问题的检测

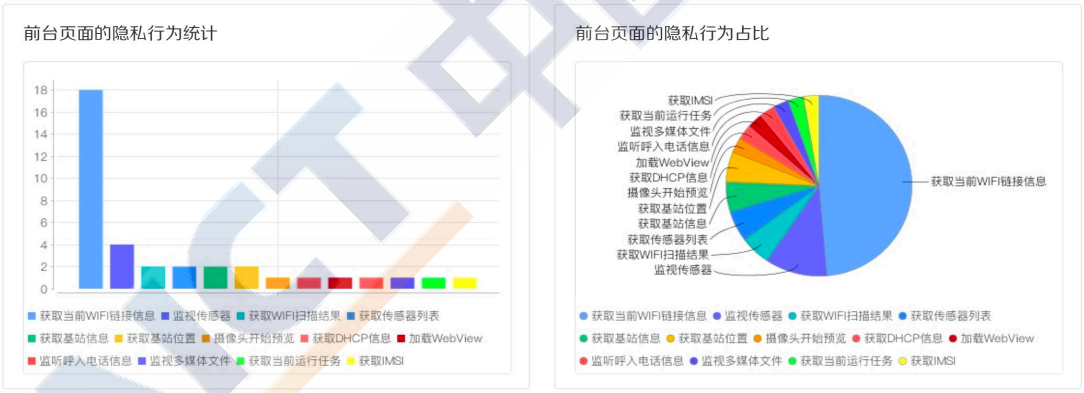
本报告针对数据违法违规使用安全问题共检测了 10 款 App，包括：金融类 4 款、在线教育类 2 款和美图娱乐类 4 款，数据违法违规使用检测项包括：静态权限检测、动态场景检测和隐私专项检测。

在静态权限检测分析中主要对App权限申请使用情况进行检测，在已检测的 6 款 App 中（加固的 App 因存在代码混淆等问题无法进行该项检测）都存在不同程度的过度申请权限，冗余权限，超范围索权等情况。

在动态场景检测分析中主要对 App 在运行使用过程中的隐私政策明示、权限使用场景、隐私行为、数据传输等方面进行了全面的检测分析。在隐私政策检测中，10 款 App 均向用户明示告知隐私政策。在权限使用场景检测中主要针对前台权限使用场景进行了检测，

其中重点针对摄像信息采集进行了检测，这 10 款 App 摄像采集权限均进行了权限申请和明示。在隐私行为检测中，根据统计数据来看针对摄像头开启权限方面未见频繁多次调用该权限，其他隐私行为调用权限的频率也均显示正常，具体隐私行为统计图如图 4 所示。在数据传输检测过程中，这 10 款 App 均存在不同程度的明文传输情况。

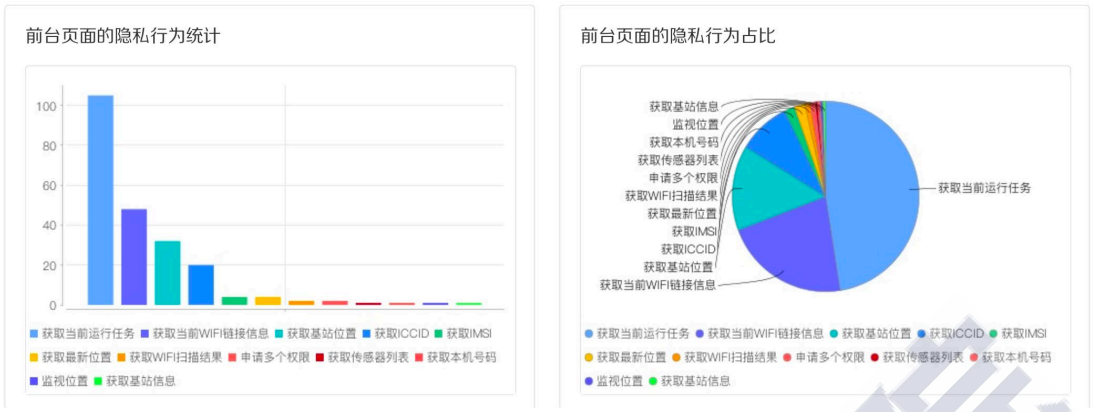
在隐私专项检测过程中，本报告主要针对未公开收集使用规则、未征得用户同意收集个人信息、一揽子授权、频繁申请权限等问题进行了专项检测。通过检测发现，1 款 App 存在未公开收集使用规则的问题，7 款 App 存在未征得用户同意收集个人信息的问题，2 款 App 存在频繁申请权限的问题。



（1） App1 隐私行为统计图



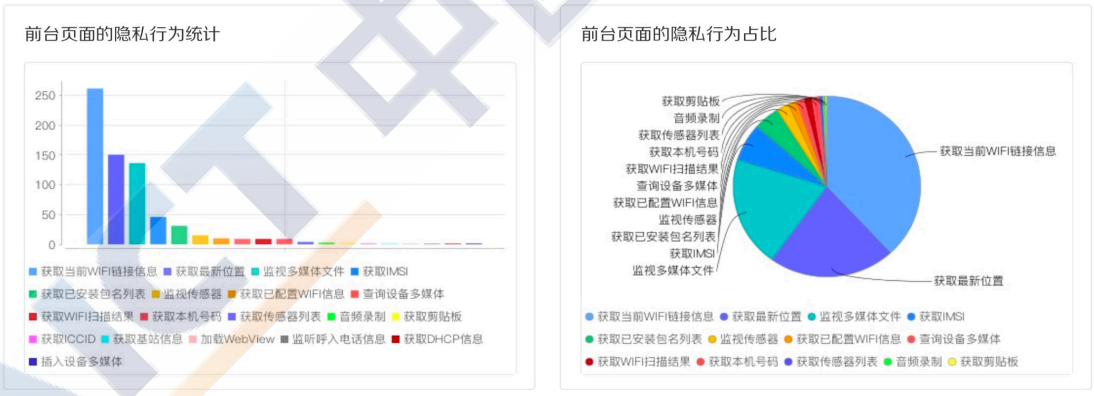
（2） App2 隐私行为统计图



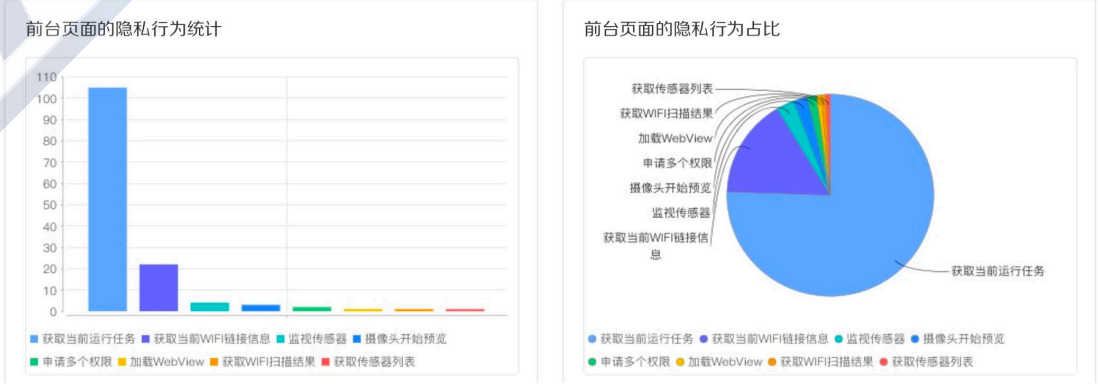
（3） App3 隐私行为统计图



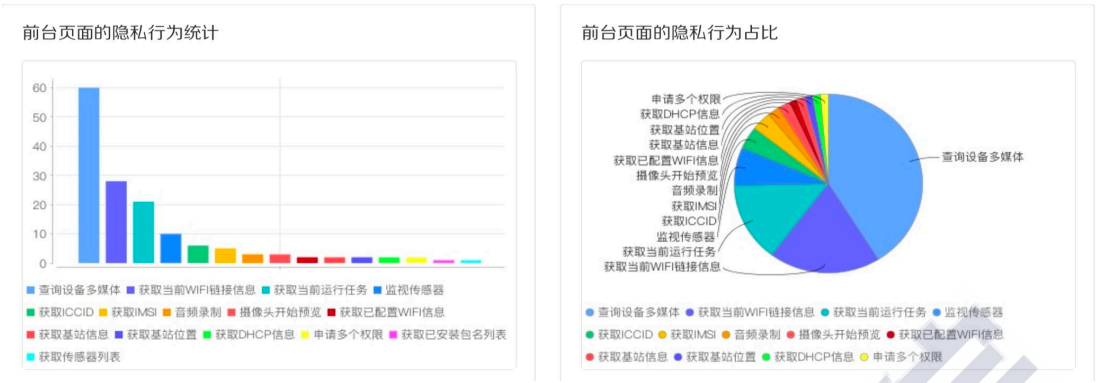
（4） App4 隐私行为统计图



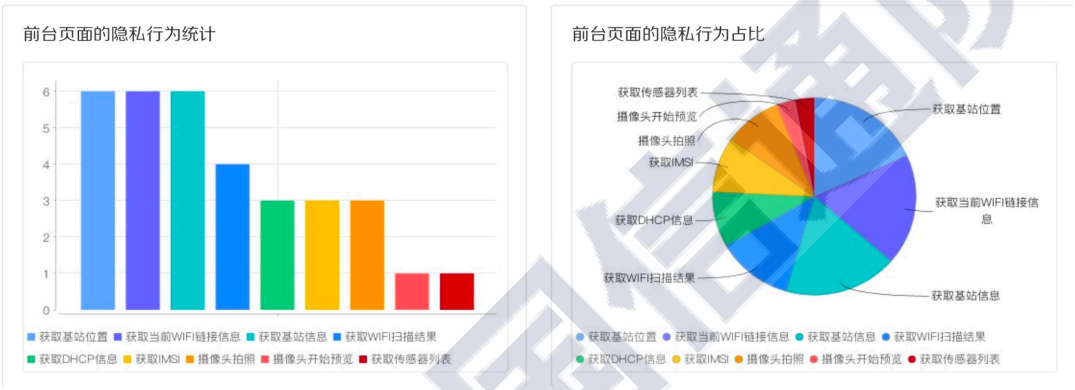
（5） App5 隐私行为统计图



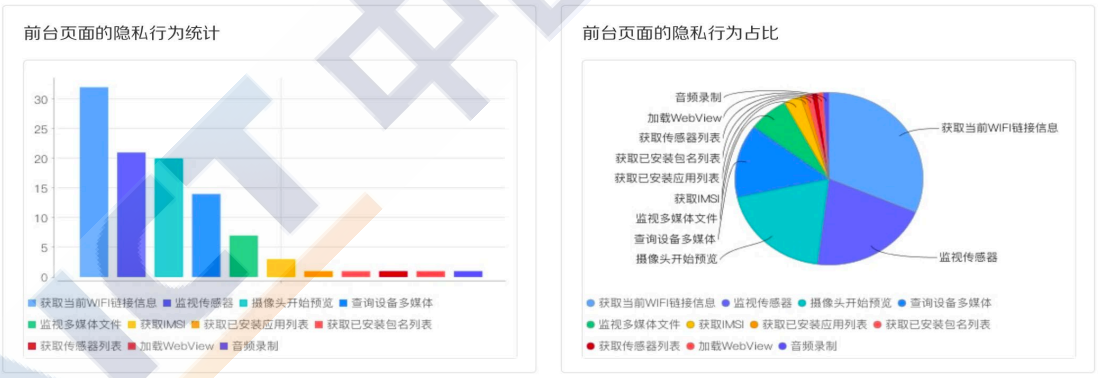
（6） App6 隐私行为统计图



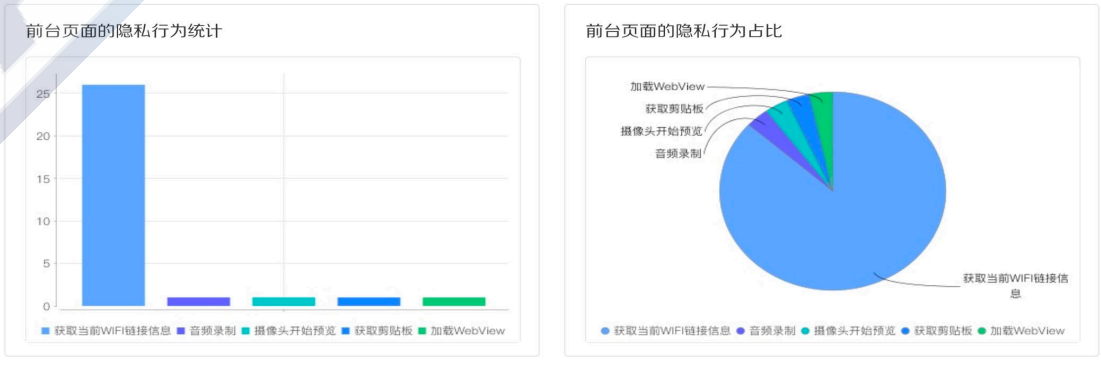
（7） App7 隐私行为统计图



（8） App8 隐私行为统计图



（9） App9 隐私行为统计图



（10）App10 隐私行为统计图

图 4　10 款 App 的隐私行为统计图

三、关于人脸深度伪造安全问题的检测

本报告针对人脸深度伪造安全问题共检测了 10 款 App，包括：智慧园区类 1 款、美图娱乐类 4 款、出行类 2 款、政府应用类 3 款。人脸深度伪造检测项包括：活体识别检测和人脸伪造安全检测。活体识别检测使用黑白照片，彩色照片，以及屏幕照片分别对人脸识别功能进行检测，共进行了 5 组测试。人脸伪造安全检查使用百度开源的人脸融合接口生成了 5 组融合图像，对人脸识别进行接口测试。通过检测发现，1 款出行类 App 可以利用黑白照片成功绕过活体识别检测;1 款政府应用类 App 可以利用屏幕视频播放成功绕过活体识别检测。

除此之外，1 款智慧园区类、1 款美图娱乐类和 1 款政府应用类 App 在人脸识别验证时需要进行眨眼动作以配合进行活体识别验证。2 款美图娱乐类 App 在人脸识别验证时需要进行眨眼、摇头、张嘴等动作以配合进行活体识别验证。2 款出行类 App 在人脸识别验证时存在错误次数太多被禁用的安全策。

免责声明

本报告主要针对截止2020年5月1日安卓应用市场的人脸识别有关的 App 安全状况进行统计、研究和分析。本报告提供给媒体、公众和相关政府及行业机构作为涉及人脸识别相关App安全状况介绍和研究资料，请相关单位酌情使用。如若本报告阐述之状况、数据与其他机构研究结果有差异，请使用方自行辨别，中国信息通信研究院安全研究所不承担与此相关的一切法律责任。因研究团队能力有限，报告仅作为参考研究，多有纰漏与不足之处，欢迎各领导专家批评指正，我们持续改进。

CAICT 中国信通院

中国信息通信研究院 安全研究所

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62308070

传真：010-62300264

网址：www.caict.ac.cn

北京百度网讯科技有限公司

地址：北京市海淀区上地十街 10 号百度大厦

邮政编码：100085

联系电话：010-59928888

传真：010-59920000

网址：www.baidu.com