CAICT 中国信通院

生物识别隐私保护研究报告

（2020 年）

中国信息通信研究院泰尔终端实验室
电信终端产业协会
中国互联网协会
互联网金融身份认证联盟
移动APP创新与个人信息保护实验室

2020 年 10 月

版权声明

本报告版权属于中国信息通信研究院、电信终端产业协会、中国互联网协会、互联网金融身份认证联盟和移动 **APP** 创新与个人信息保护实验室，并受法律保护。转载、摘编或利用其它方式使用本报告文字或者观点的，应注明“来源：中国信息通信研究院、电信终端产业协会、中国互联网协会、互联网金融身份认证联盟和移动 **APP** 创新与个人信息保护实验室”。违反上述声明者，将追究其相关法律责任。

前　言

当前，世界正处于新一轮科技革命和产业革命的变革浪潮中，以智能终端为代表的互联网产业已成为“互联网+”的基础设施，是推动经济社会变革的重要力量。近年来，越来越多的智能终端及应用软件搭载生物识别技术，在金融科技、安防、民生、智慧家庭等领域广泛应用，为用户带来了更加便利的体验。随着产业的蓬勃发展，生物识别产业未来会进一步走向信息化、智能化。

目前，频频出现的用户个人信息泄露事件表明，以指纹、人脸、声纹、步态等为代表的个人生物识别信息作为高度敏感的用户个人信息，存在一定的隐私泄露和信息安全风险。为研究生物识别隐私保护方面的风险和应对措施，维护用户合法权益，中国信息通信研究院泰尔终端实验室、电信终端产业协会、中国互联网协会、互联网金融身份认证联盟和移动 APP 创新与个人信息保护实验室联合制定与发布本报告。本报告着眼于生物识别产业现状，基于国内外相关法律法规和标准规范，阐述生物识别隐私保护面临的挑战，在设备、应用、算法等方面提出对生物识别信息的保护要点，并倡议产业界落实企业主体责任，加强行业自律，强化产业协作体系，共筑生物识别隐私保护的良好生态。

目 录

一、 生物识别产业现状 1

（一）生物识别产业市场现状 1

（二）生物识别产业发展趋势 2

（三）生物识别隐私保护监管动态 3

二、 生物识别隐私保护面临的挑战 6

（一）特定生物识别模态信息保护缺少明确标准 7

（二）生物识别信息过度收集使用难识别难举证 7

（三）设备及应用抵抗呈现攻击的水平参差不齐 7

（四）深度伪造生物识别信息难判定、难追溯 9

（五）生物识别算法缺陷引发高误识率 10

（六）传感器数据缺乏权限保护 10

（七）生物识别模型面临窃取风险 11

（八）供应链安全导致隐私泄露风险 11

三、 生物识别隐私保护要点 12

（一） 落实规定要求，及时自查自纠 12

（二） 对接国际规范，输出中国方案 12

（三） 健全标准体系，完善评价指标 13

（四） 提升安全能力，落实告知同意 13

（五） 构建评估机制，提升保护力度 13

（六） 加强技术研究，创新技术手段 14

（七） 赋能技术落地，推动产业升级 14

（八） 制定保护机制，完善供应链管理 14

四、 生物识别隐私保护行动倡议 14

（一） 加强行业自律，明确企业主体责任 15

（二） 依托公众监督，及时响应用户关切 15

（三） 规范信息共享规则，明确责任归属 16

（四） 规范推送及权限调用，加强用户可知可控.....16
（五） 提高应用防护能力，保障用户合法权益.....16
（六） 规范平台信息声明，保证下载用户知情.....17
（七） 完善安全审核职责，落实分发上架机制.....17
（八） 鼓励各方合作共享，强化产业协作体系.....17

CAICT 中国信通院

一、生物识别产业现状

（一）生物识别产业市场现状

全球生物识别产业近年来稳步增长。自 2010 年以来，全球生物识别产业迅速增长，根据国际生物识别集团（IBG）和美国咨询机构 Transparency Market Research 数据显示，在 2017-2018 年，市场增速最快，增长率达到 22.28%；在 2019 年之后呈现逐步平稳增长的趋势，至 2020 年将达到 233 亿美元。

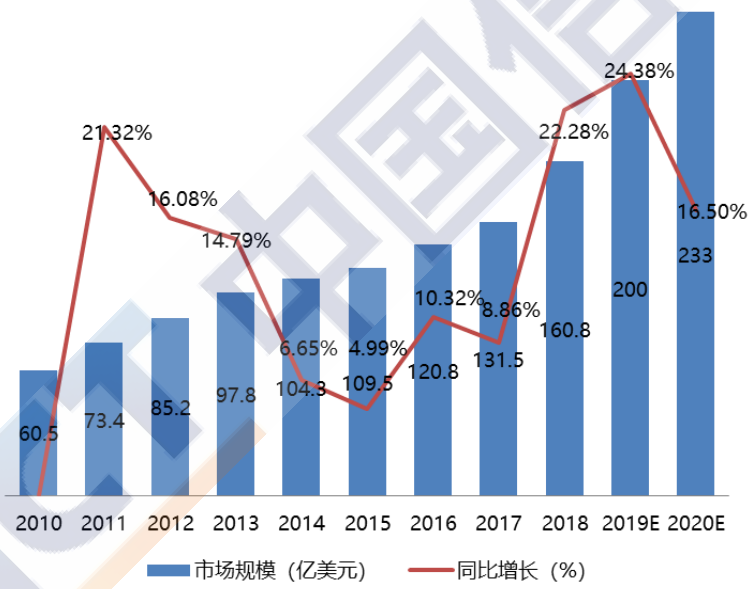

图 1 全球生物特征识别技术市场规模

北美亚太在全球生物识别市场占比居前两位。根据 IBG 最新报告显示，在生物识别产业中，北美地区占比居首，达到 33.5%；其次是亚太地区，为 23.8%；欧洲、中东和印度、中南美洲、非洲地区，市占率依次为 16.5%、11.0%、9.1%和 6.1%。美国是全球主要的生物识别市场 ，“911”事件发生后，全美在 115 座机场和 14 个主要港口

设立了“美国访客和移民身份显示技术”系统，采用指纹识别、人脸识别与虹膜识别等技术验证访客与移民信息；同时 27 个免签国公民去往美国，都必须持有生物识别护照。

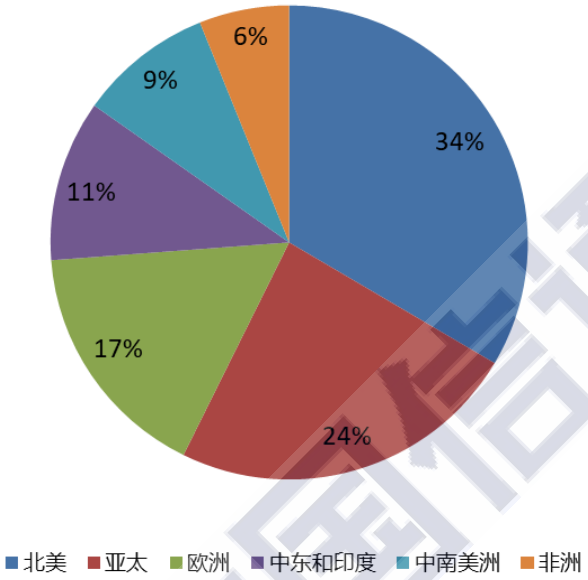

图 2 全球生物特征识别市场占比

（二）生物识别产业发展趋势

近年来，我国生物特征识别产业发展迅速，产业链基本形成，市场规模快速增长，指纹识别所占份额仍处于高位，人脸识别市场规模不断扩大，各类生物识别市场蓬勃发展。我国移动终端生物特征识别发展呈现如下特点：

新技术不断涌现和落地，为生物识别带来技术突破。以深度学习为代表的新技术与生物识别技术的融合，使识别技术不断出现新突破，识别的准确度大幅提高。

生物识别技术逐渐成熟，应用场景趋于复杂多样化。不同应用场景，对识别技术的需求有所差异，针对不同的场景使用不同的识别技

术、或结合多种识别技术于一体，为不同的领域、行业、场景、应用提供定制化的识别技术，是生物识别技术产业未来发展的趋势。近年来，随着声纹、掌纹、静脉等识别技术取得重大突破，其产品得到了广泛的应用。未来，生物特征识别技术也将继续多元化发展。

多生物特征融合技术广泛应用，以提升识别系统的安全与体验。由于客观条件变化的不可估计性，单生物特征识别技术往往会遇到难以克服的特例。而且在安全性要求极高的应用领域，单生物特征识别的性能很难达到预期的效果。因此，多生物特征识别技术越来越受到人们的关注。多生物特征识别技术利用了多个生物特征，结合数据融合技术，不仅提高了识别的准确性，而且扩大了多生物特征识别系统的应用范围，降低了多生物特征识别系统风险，是未来生物特征识别应用领域的趋势。

融合技术将引领产业升级，带来数字化新体验。5G、人工智能、大数据、云计算、AR 等技术与生物识别的结合应用，使新需求和新愿景可以落地实现，赋能垂直行业，进一步引领产业升级，带来全息影像通话、可穿戴设备生物特征身份识别、基于眼球追踪的广告分析等应用场景。

（三）生物识别隐私保护监管动态

当前，世界主要国家高度重视对生物识别信息的保护，相关法律法规制定以及标准化工作有序开展。

欧美等国：立法先行，监管打击并举。欧美等地区对于生物特征信息保护的立法、实践较为完善，内容全面且具体，特别是美国相关

的立法原则，目前成为全球其他大多数国家、地区和国际组织的参考原则。

美国伊利诺伊州于 2008 颁布的《生物信息隐私法案》（BIPA），是美国境内第一部规范生物标识和生物识别信息的收集、使用、保护、处理、存储和销毁的法律。2018 年 6 月 28 日，加州颁布了《2018 年加州消费者隐私法案》（CCPA），旨在加强对用户生物信息等隐私数据的安全保护，该法案于 2020 年 1 月 1 日起正式实施。2019 年 5 月，旧金山通过了《停止秘密监视条例》，全面禁止市政府使用人脸识别技术，以防公权力机构的监视网络侵犯个人隐私及其他权利。2019 年 6 月 28 日，两党议员分别在众议院、参议院同时提出的《2019 年深度伪造报告法案》（Deepfakes Report Act of 2019）要求国土安全部商有关部门对不断增长的深度伪造技术开展前瞻性研究，以评估防范这项新技术可能带来的风险及构成的威胁。

欧盟于 2018 年 5 月 25 日起正式施行《通用数据保护条例》（GDPR），赋予欧盟用户控制个人数据的权利，明确给出了生物识别信息的定义，成为各国制定个人信息保护法案的重要参考。随后，印度、巴西等国家纷纷制定了数据保护的法律，对个人数据的收集和使用进行了明确规定。GDPR 已引发全球立法规则进一步融合，同时，GDPR 执法案例也成为监管态势的重要参照。自 GDPR 实施以来，欧盟已开具数百项罚单，对象包括英国航空、谷歌、万豪国际集团等企业和个人。

国内：法律法规不断完善，标准体系初步形成。2009 年，刑法

修正案（七）首次将窃取或以其他方式非法获取公民个人信息情节严重的行为规定为犯罪。2012 年，《全国人民代表大会常务委员会关于加强网络信息保护的决定》规定了网络服务提供者在收集、使用、保管公民个人信息中应当遵循的原则、承担的义务及法律责任。2016 年，《中华人民共和国网络安全法》奠定了我国网络空间安全治理的法治化的基础，不仅明确地界定了个人信息的含义，把个人生物识别信息纳入个人信息的范畴，同时还对个人信息的收集、存储、保管和使用进行了更详细、全面的规范，提出了“最少够用原则”，并规定了信息权利人删除权、知情权、更正权等。2020 年，《民法典》人格权编加大了对公民隐私权的保护力度：完善个人信息的法律定义；明晰处理个人信息内涵、原则和条件；严格限制处理个人信息免责事由；保障信息主体的更正权与删除权；强化处理者的信息安全保障义务；明确机关、机构及人员的保密义务。2013 年，工业和信息化部第 24 号令《电信和互联网用户个人信息保护规定》，电信业务经营者、互联网信息服务提供者在提供服务的过程中收集、使用用户个人信息，应当遵循合法、正当、必要的原则。2020 年 7 月 3 日，《数据安全法（草案）》正式向社会公开征求意见，规定了“数据处理者的数据安全保护义务”，明确规定了任何组织、个人收集数据，必须采取合法、正当的方式，不得窃取或者以其他非法方式获取数据，不得超过法律、行政法规规定的必要限度。与此同时，《个人信息保护法》也在制定过程中。

2020 年，《信息安全技术 个人信息安全规范》正式发布，并于

2020 年 10 月 1 日实施。《规范》继续沿用了 2017 版的七大原则，分别是：权责一致原则、目的明确原则、选择同意原则、最少够用原则、公开透明原则、确保安全原则、主体参与原则。对于个人生物识别信息，《规范》明确了在收集、存储和披露等环节的规定。

目前全国信息安全标准化技术委员会、中国通信标准化协会、电信终端产业协会等标准化组织和产业协会正在推进以指纹识别、人脸识别、声纹识别、步态识别、语音识别以及基因识别为代表的生物识别安全技术与信息保护的标准化工作，生物识别隐私保护的标准体系已初步形成。以互联网金融身份认证联盟（IIFAA）联盟为代表的国内产业联盟发展迅猛，同时，各大国内企业、科研机构也在积极参与国际生物识别相关标准的制定，如：由蚂蚁集团牵头的 ISO/TC68《移动金融服务客户身份鉴别指南》（ISO/NP5158）于 2020 年立项成功，各类标准的研制与落地实施将进一步完善标准体系。

二、生物识别隐私保护面临的挑战

随着生物识别信息的大规模应用，用户隐私与安全保护问题逐渐暴露，引发在用户个人信息收集和使用方面的风险。生物识别信息与个人身份高度绑定，且具有不易变更的特点，生物信息泄露、信息缺乏授权、深度伪造等问题严重威胁了广大用户的切身利益，生物识别信息的滥用将带来严重的社会问题。移动互联网产业生物识别隐私保护工作面临严峻的挑战。

（一）特定生物识别模态信息保护缺少明确标准

特定生物识别模态信息采集、数据传输的保密性和完整性以及存储缺乏明确标准。目前指纹、人脸、虹膜、声纹、静脉、步态、基因等生物识别模态均得到不同程度的应用，涵盖各行各业的应用场景。不同模态特点、不同应用场景对于生物识别信息保护的要求存在差异，亟需针对特定生物识别模态提出相应规范。目前全国信息安全标准化技术委员会、中国通信标准化协会、电信终端产业协会等标准化组织和产业协会正在推进以指纹识别、人脸识别、声纹识别、步态识别以及基因识别为代表的生物识别安全技术与信息保护的标准化工作，相关标准的研制将一定程度解决产业中面临的标准缺失问题。

（二）生物识别信息过度收集使用难识别难举证

设备或应用在用户不知情的情况下，违规处理生物识别信息。用户生物识别信息，如语音信息、健康信息等，在不知情的情况下被收集使用，以用户可感知的方式呈现。但信息是如何被收集、通过何种渠道共享传播，普通用户难识别、难举证。较多应用并未通过隐私政策或其他途径告知用户收集使用信息的目的、方式和范围，也未向用户提供明确的允许和拒绝的选择，这种累积性的权益侵害在日常生活中普遍存在，引发了用户的严重担忧，生物识别信息过度收集使用的乱象亟待解决。

（三）设备及应用抵抗呈现攻击的水平参差不齐

呈现攻击（Presentation Attacks）一直是生物识别技术所面临的

主要安全风险，呈现攻击检测（Presentation Attack Detection，PAD）技术也是生物识别系统进入高端、安全、大规模应用的最大瓶颈。呈现攻击的方式具有多样性的特点，以人脸识别应用为例，呈现攻击的方式大致可以分为：二维呈现攻击，包括二维静态纸制与电子照片，二维动态图像、视频；三维呈现攻击，包括三维面具攻击和高精度的三维头模攻击。各类型的攻击方式的攻击成本，检测的难易程度，攻击的出现频率也存在很大差异。在生物识别技术大规模应用中，受制于相关硬件及不同的算法能力差异，不同产品抵抗呈现攻击的能力参差不齐。

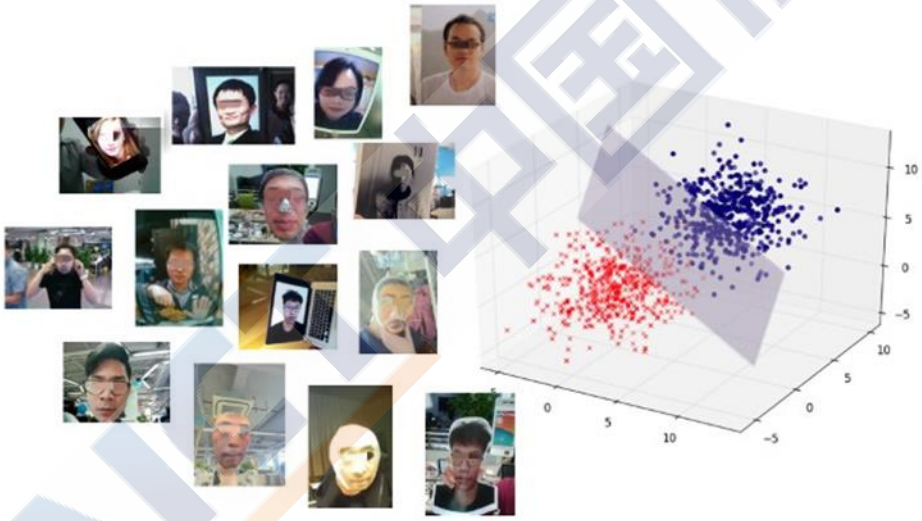

图 3 不同类型针对人脸识别的呈现攻击方式

以人脸识别为例，PAD 技术是一个重要的算法领域。当用户发起人脸识别请求时，算法需要判断此次生物特征来源于真人还是某类型呈现介质。PAD 技术基于不同的传感设备，可以划分为不同数据模态的检测算法。其中常见的包括基于 2D 摄像头的单 RGB 假体检测算法，基于 3D 摄像头的 3D 深度假体检测算法和基于近红外摄像头的

近红外假体检测算法。由于假体呈现的介质具有不同特点，相应每一类型的 PAD 算法所覆盖的攻击方式也有所不同。

移动端设备广泛采用 2D 摄像头进行人脸识别，缺乏 3D 信息，对于部分制作精良的人脸假体攻击的防范能力较弱。通过 2D 单模态进行高安全能力的呈现攻击检测需要很高的技术门槛。此前，在业界暴露出的呈现攻击安全事件大多数是突破 2D 活体检测算法引起。对于高安全需求的移动终端、IoT 设备，由于集成了 3D 深度、近红外传感器，可以通过多维度数据辅助进行呈现攻击检测，大大降低假体攻击的安全风险。

（四）深度伪造生物识别信息难判定、难追溯

AI 换脸应用的爆红，引发公众对生物识别安全等问题的担忧。同时，这类深度伪造生物信息的应用存在隐私风险。

经过深度伪造的生物识别信息难以判定。各类“换脸”技术制造了大量的虚假视频，目前利用 AI 技术换脸的黑产已经在国内形成了完整的产业链，从下游成品情色视频、中游定制视频到上游软件及教程都有提供，大大降低了技术门槛与造假成本。同时，AI 语音伪造技术近年来越来越多地被用来进行电信诈骗，引发了强烈的社会反响。深度伪造技术与“反伪造”技术处于攻防拉锯状态，双方技术均在高速发展中，针对深度伪造生物识别信息的判定尚无成熟的判定手段与依据。

深度伪造生物识别信息大量传播，难以追溯。目前尚无对深度伪造生物识别信息的标识类要求，对传播的信息难以进行追溯。尤其是

针对政客、明星等的伪造视频，将带来负面的社会影响，引发社会恐慌。

（五）生物识别算法缺陷引发高误识率

近年来，对生物识别算法的攻击事件时有发生，各类新兴的生物识别技术也面临着算法缺陷引起的误识事件。2019 年 1 月，在德国莱比锡召开的黑客组织 Chaos Computer Club 年度大会上，德国安全研究员 Jan Krissler 和 Julian Albrecht 演示了利用照片制成手模绕过了基于静脉的身份验证。2019 年 3 月，攻击者利用 AI 技术成功模仿并冒充英国某能源公司在德国母公司 CEO 的声音，包括特殊的德国口音，诈骗了 22 万欧元。频频出现的安全事件表明，生物识别算法仍然存在各种各样的缺陷，比如，指纹图像处理过程中前景与背景分割不完善，使得原属于背景的信息被混叠入前景中，被当作指纹特征参与了匹配运算，进而导致了攻击事件的发生，生物识别算法仍需持续改进。

（六）传感器数据缺乏权限保护

各类应用加速向垂直行业渗透，具备收集心率、血氧饱和度等功能的传感器已在多款智能终端搭载使用，激光雷达等专业传感器也逐渐搭载到智能音箱设备用来实现手势交互等功能。

设备与应用普遍缺乏对传感器数据的保护机制。目前多数的智能终端操作系统对诸多传感器缺乏权限管理，任意应用可以随意调用部分传感器数据，面临数据泄露的风险。

传感器性能与 AI 技术的提升，使传感器数据被用来恢复用户的语音信息等。基于生物特征传感器、运动传感器、环境传感器和位置传感器的数据将直接或间接进行生物识别信息的采集和分析，来自浙江大学的最新研究成果表明， 可利用手机内置加速度传感器采集手机扬声器所发出声音的震动信号，实现对用户语音的窃听。随着传感器精度与采集频率越来越高，这类数据如被恶意应用获取，将引发用户个人身份信息泄露的风险。

（七）生物识别模型面临窃取风险

针对机器学习模型的攻击手段层出不穷，给生物识别模型安全带来严重的安全隐患。虽然对机器学习模型的加固已有很多成熟的解决方案，但攻击者可以采用如：对抗样本导致模型策略失效；在模型训练过程中通过数据投毒（污染训练数据）从而影响最终的模型效果；或者是通过黑盒探测的方式，实现对算法模型的窃取，严重影响了模型的可用性和安全性。对生物识别模型的攻击，使得模型信息（例如模型结构与模型参数）泄露，可能导致算法的数据被逆向还原，进而造成严重的信息泄露，引发业务、资产安全风险。

（八）供应链安全导致隐私泄露风险

引入第三方母模型构建生物识别算法子模型，或面临供应链安全风险。受训练数据规模、训练机器资源等限制，目前很多厂商会利用第三方大规模数据训练后的模型作为母模型，并结合自身产品或者特定场景的少量数据做模型微调，将微调后的模型应用在商业产品中。

第三方母模型普遍缺乏严格的测试管理和安全认证，存在未知安全漏洞。攻击者可以利用特殊的攻击手段，如：抗拒样本攻击，窃取或篡改用户的生物识别隐私信息或模型数据。同时，如果母模型供应方人为在母模型中预置后门，将存在更大的安全风险。

三、生物识别隐私保护要点

随着互联网的迅猛发展，终端功能日益丰富，在给用户生活带来极大便利性的同时，也逐步成为绑定了大量个人信息的载体，带来诸多安全威胁。我国作为数字经济大国和生物识别应用最广泛的国家之一，应进一步提升行业对生物识别隐私保护的水平，保障用户合法权益，促进行业健康发展。

（一）落实规定要求，及时自查自纠

强化落实生物识别隐私保护相关法律法规与标准要求。将法律法规和标准要求落实到企业管理制度，及时自查自纠，同时畅通用户投诉渠道，完善投诉处理服务机制和流程。

（二）对接国际规范，输出中国方案

提升国际的标准化水平，贡献中国力量和方案。组织国内企业、科研院所等多方力量加强研究储备，在 IEEE、ISO/IEC、ITU 等国际标准化组织中联合发声，提出生物识别隐私保护相关提案，贡献更多中国力量和方案，实质性主导和参与生物识别隐私保护相关国际标准工作。

（三）健全标准体系，完善评价指标

完善我国的生物识别隐私保护标准体系，加快重点标准研制。在我国现有的个人信息保护、生物识别安全等标准体系框架下，加快研制生物识别隐私保护等相关标准，制定完善的标准推进计划，推进生物特征识别安全规范等产业急需的标准研制工作，强化标准应用实施，形成并完善生物识别隐私保护评价指标体系。

（四）提升安全能力，落实告知同意

提升设备可知可控能力；规范告知明示内容，确保用户知情权、选择权。终端设备应遵循行为与用户意愿一致的基本原则，设计完善的权限管控机制，提升用户可知可控的能力，避免用户生物识别隐私信息泄露。终端设备和移动应用在收集和使用生物识别隐私信息时，应详细告知所收集生物识别信息的内容、目的、方式、范围、频次、保护措施以及公开、转移、共享等相关信息。遵循告知同意原则，在收集用户个人信息前，以易于感知的方式，明示告知用户收集使用规则，待用户同意后，方可执行。

（五）构建评估机制，提升保护力度

开展检测评估，提升对生物识别隐私的保护。依托行业组织和第三方机构，共同构建生物识别隐私保护检测评估平台，制定生物识别产品、应用和服务的隐私安全检测评估方法和指标体系，研发安全检测评估工具集，通过测试验证提升生物识别产品、应用和服务的安全性，降低隐私泄露的风险。

（六）加强技术研究，创新技术手段

创新生物识别隐私保护技术手段，加强基础理论研究和技术研发。引导产学研各界联合开展生物识别技术的研究：不断提升生物识别算法性能和安全性，改善算法缺陷，增强生物识别算法活体检测能力，减少攻击面；创新生物识别隐私保护手段，强化对生物识别隐私保护理论的研究，加强生物识别信息匿名化、同态加密、差分隐私等核心方向和技术的研究，提升生物识别隐私的保护能力。

（七）赋能技术落地，推动产业升级

鼓励隐私保护与安全新技术的应用推广，推动实现产业升级。鼓励产业链各方积极将可信技术、零知识证明、多方计算等隐私保护与信息安全的技术应用到研发、生产等实践环节，进一步推动技术落地和产业升级。

（八）制定保护机制，完善供应链管理

制定生物识别相关的供应链保护机制，完善相关管理制度。企业应制定并不断完善供应链审查及安全保护机制，提升产业链相关厂商在研发、交付、使用等环节的隐私保护要求和安全对抗能力，从源头加强对生物识别隐私信息的安全保护。

四、生物识别隐私保护行动倡议

提升移动互联网产业生物识别隐私保护能力，加强用户权益保护，离不开全行业的共同努力。在工业和信息化部指导下，中国信息通信研究院秉持“国家高端专业智库，产业创新发展平台”的发展定位，

对群众生活密切相关、下载使用量较大、用户投诉多的 APP，持续支撑开展大量技术检测和检查工作。并联合行业协会、互联网企业在制定规范、签署行业自律公约等方面进行了有益的探索，在加强用户个人信息保护，保护人民群众的切身利益方面取得了积极成效。在此基础上，我们倡议：

（一）加强行业自律，明确企业主体责任

严格遵守法律法规，全面加强行业自律。行业自律是生物识别隐私保护的关键，也是企业可持续发展的内在基础。鼓励在行业协会的组织下，严格遵守法律法规，积极开展自律工作。终端厂商、分发平台、应用开发者积极落实主体责任，主动适应个人信息保护和数据管理新形势新要求，严格遵守法律法规，贯彻落实个人信息收集使用规定，提升对生物识别隐私信息的保护力度，不断完善企业内部的个人信息保护和数据管理制度，持续优化用户隐私政策，并将个人信息保护的要求贯彻执行到规划、开发、运营等各个环节，积极配合主管部门的监管要求，切实有效维护好用户合法权益。

（二）依托公众监督，及时响应用户关切

高度重视用户权益保障，为用户举报监督创造便利条件。公众监督是保障用户权益的重要渠道，也是约束企业行为的有效方式。终端厂商、分发平台、应用开发者应以用户为中心，为用户举报投诉设置便捷的方式和渠道，健全公众参与监督的机制，时刻关注用户感受和

体验，尊重并保障用户的投诉权和可追溯权，积极向行业主管部门移交公众举报信息。

（三）规范信息共享规则，明确责任归属

根据信息共享和责任归属原则，增加信息可追溯性。生物识别信息的应用企业应制定清晰、明确的信息共享规则，在转移、共享用户生物识别信息前，应先明示用户共享的内容、共享对象、共享用途等相关信息，征得用户同意后，方可转移或共享信息。应与信息接收方订立安全协议，明确各方信息保护责任，并要求信息接收方依规执行。

（四）规范推送及权限调用，加强用户可知可控

加强应用推送及权限调用管理，净化应用环境。完善的应用推送及权限调用管理机制可以有效约束应用服务在未向用户告知，或未以显著方式标示情况下，将收集到的生物识别信息、用户搜索、浏览记录、使用习惯等个人信息，用于定向推送或精准营销的行为。构建应用服务合规合理定向推送，净化移动互联网应用环境，提高公众对应用服务的使用信心。

（五）提高应用防护能力，保障用户合法权益

提高安全专业能力，高度重视生物识别隐私保护。安全防护能力是保护用户生物识别隐私信息的基础保障。移动应用开发者应遵循“最小必要”原则，采取必要的手段保障应用的安全性和用户数据的机密性、完整性和可用性。应用服务开发者应将安全编码原则贯穿整个软件开发周期，采用高等级 API 和安全 SDK、适配最新操作系统及

外部代码库、尽量减少代码的攻击面。并对应用进行必要的安全加固、采用安全存储和传输技术保障用户敏感信息安全，通过完善的身份认证机制保障通信过程安全。

（六）规范平台信息声明，保证下载用户知情

为用户提供应用详情，增加应用环境透明度。应用平台信息声明是用户了解应用基本信息的重要途径。平台应明示用户，应用名称、功能描述、卸载方法、开发者信息、应用安装及运行所需权限列表等，明确告知用户应用收集使用用户个人信息的内容、目的、方式和范围等。在用户下载应用时，应明示应用名称、功能描述、卸载方法、开发者信息、应用安装及运行所需权限列表等，应明示用户收集使用个人信息的内容、目的、方式和范围。

（七）完善安全审核职责，落实分发上架机制

通过应用检查审核机制，为用户提供合规应用。应用分发平台审核机制是保证用户个人信息的基础保障。平台应审核开发者资质和应用相关信息。平台应制定明确的上架要求并建立完备的检测机制，通过自动化检测和人工审核手段，对应用收集使用用户个人信息的行为进行规范。应用分发平台应对应用进行跟踪监测，包括定期复查，定期对已上架的应用进行复查，发现问题立即下架。

（八）鼓励各方合作共享，强化产业协作体系

针对焦点和难点问题，产业界齐心协力联手行动。针对当前用户普遍关注的生物信息过度收集使用等问题，积极响应产业诉求，加强

终端厂商、应用开发等多环节的沟通协调，在权限管理、告知同意、设备识别码防护等多方面加强协作，制定行业标准规范，研制技术方案，开发检测手段。在检测认证、监测处置等方面协调统一行动，强化产业协作体系，提升生物识别用户隐私与安全保护能力，全面加强用户权益保护。

CAICT 中国信通院

免责声明

本报告内容供相关单位参考，酌情使用。若本报告内容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、电信终端产业协会、中国互联网协会、互联网金融身份认证联盟和移动 **APP** 创新与个人信息保护实验室不承担与此相关的一切法律责任。因研究团队能力有限，报告内容多有不足之处，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 泰尔终端实验室

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62300479

传真：010-62304980

网址：www.caict.ac.cn