ICS 33.050
CCS M 30

团　体　标　准

T/TAF 077.3-XXXX

APP收集使用个人信息最小必要评估规范 第3部分：图片信息

Application software user personal information collection and usage minimization and necessity evaluation specification— Part 3: Image file

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

电信终端产业协会　发布

目　　次

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。

本文件是T/TAF 077《APP收集使用个人信息最小必要评估规范》的第3部分。T/TAF 077已经发布了以下部分：

——第1部分：总则；
——第2部分：位置信息；
——第4部分：通讯录；
——第5部分：设备信息；
——第6部分：软件列表；
——第7部分：人脸信息；
——第8部分：录像信息；
——第9部分：短信信息；
——第10部分：录音信息；
——第11部分：通话记录；
——第12部分：好友列表；
——第13部分：传感器信息；
——第14部分：应用日志信息；
——第15部分：房产信息；
——第16部分：交易记录；
——第17部分：身份信息。

本文件代替T/TAF 077.3-2020《APP收集使用个人信息最小必要评估规范 图片信息》，与T/TAF 077.3-2020相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 将权限授权的要求从收集阶段中提出单独小节，将原收集阶段的告知同意小节的内容改为收集阶段要求；
b) 优化并完善了在存储阶段图片信息最小必要的要求；
c) 针对一些热点事件中问题，修改了在删除阶段图片信息最小必要的要求；
d) 增加了评估方法章节，并完善了评估流程。

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。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、OPPO广东移动通信有限公司、华为技术有限公司、北京奇虎科技有限公司、高通无线通信技术(中国)有限公司、北京字节跳动科技有限公司、北京三星通信技术研究有限公司、荣耀终端有限公司、北京快手科技有限公司。

本文件主要起草人：李腾、王艳红、杨明慧、宁华、常新苗、刘陶、武林娜、付艳艳、杜云、毛欣怡、王江胜、衣强、姚一楠、王宇晓、苏翔、杨骁涵、吴越、赵晓娜、落红卫、刘林汶、游苏英、安潇羽、宋恺、卜英华。

引　　言

随着移动移动互联网的迅速发展和日益成熟，移动智能终端功能的成熟与便利，可以让人们随时随地发现并分享身边的美好事物，形成图片信息。这些信息除了照片中的拍摄的内容，还有可能是拍摄图片时的精准定位信息、照片中的人脸信息或者指纹信息、屏幕截图等个人信息等。然而，在APP收集使用图片信息的过程中，有些个人信息可能并非个人信息主体使用该功能时所必须的。

本文是APP收集使用个人信息最小必要评估规范系列标准中的图片信息部分，旨在对移动互联网行业收集使用个人信息主体图片信息进行规范，落实最小、必要的原则，进一步促进移动互联网行业的健康稳定发展。

APP收集使用个人信息最小必要评估规范 第3部分：图片信息

1 范围

本文件规定了在移动应用软件在处理涉及个人信息主体个人信息相关图片信息的收集、存储、使用、删除等活动中的最小必要信息规范和评估方法，并通过对在个人信息处理活动中的典型应用场景来说明如何落实最小必要原则。

本文件适用于移动互联网应用软件提供者规范个人信息主体个人信息（图片信息）的处理活动，也适用于主管监管部门、第三方评估机构等组织对移动互联网应用程序收集图片信息行为进行监督、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 信息安全技术个人信息安全规范

T/TAF 077.1 APP收集使用个人信息最小必要评估规范 总则

3 术语和定义

GB/T 35273和T/TAF 077.1和T/TAF 077.7界定的术语和定义适用于本文件。

4 缩略语

下列缩略语适用于本文件。

APP：应用软件（Application）

GNSS：全球卫星导航系统（Global Navigation Satellite System）

5 基本原则

应满足T/TAF 077.1 《APP收集使用个人信息最小必要评估规范 总则》中的最小必要原则。

6 图片信息分类

图片可以通过拍照、屏幕截图以及对图片的再加工的方式生成。根据图片信息中包含的内容，可将图片信息分为以下三类：

a） 图片基本信息：指图片的基本特征信息，包括图片内容信息（原始的和编码后的二进制码）、图片格式、大小、分辨率；

b） 图片附加信息：拍照时间、拍照设备、拍照参数、图片名称等可关联出个人的图片信息；

c） 图片位置信息：指拍摄图片时的精准定位信息。例如安卓系统可通过 GpsLocationProvider 来获取精确位置信息。

7 图片信息典型使用场景

图片信息的收集使用包括但不限于以下场景：

a） 社交类：个人信息主体通过 APP 发送固定数量的图片到明确的一个或多个好友或朋友圈限定范围的场景。

b） 媒体发布类：个人信息主体出于图片公开的目的将图片通过 APP 发布到媒体平台的场景。

c） 图片加工类：个人信息主体通过 APP 对图片进行编辑生成新的图片的场景。

d） 图像识别类：个人信息主体通过 APP 对图片或扫一扫生成的缓存图片进行识别的场景。

e） 云盘备份类：通过 APP 将本地图片备份到云盘的场景。

f） 客服/售后类：个人信息主体在 APP 中因某种诉求发送图片到客服或售后的场景。

8 图片信息的最小必要评估要求

8.1 权限授权

APP收集图片信息主要通过调用移动智能终端的拍照或屏幕截图功能生成图片信息，或是通过读取、写入等方式访问移动智能终端上的图片信息时，应征得个人信息主体对相应权限的授权同意。APP首次使用，在媒体库中生成图片或访问图片时需要通过权限授权，在个人信息主体同意授权之前，不应生成或访问图片信息。以下表1列出了生成或访问图片时所必须的权限，非必要权限应在业务场景发生前向个人信息主体申请对应的权限。

表 1 生成或访问图片时最小必要权限

图片生成或访问方式	对应权限	用途	是否必要
拍照	相机	拍摄照片，生成图片	是
	位置	拍照时的图片定位信息	否
屏幕截图	屏幕截图(注:如系统无对应权限，应征得个人信息主体授权)	屏幕截图，生成图片	是
读取媒体库	存储权限	读取图片	是
写入媒体库	存储权限	将图片的信息写入到媒体库中	是

8.2 收集阶段

移动应用软件收集图片信息前，应告知业务功能收集使用图片信息的目的、方式和范围，并获得个人信息主体明确的授权同意。宜逐一列出该应用（含委托的第三方或嵌入的第三方SDK、插件等）不同场景中收集使用（或委托使用）图片信息的目的、方式、范围和频率，以及图片信息存储的地域、期限、超期处理的方式，采取的数据安全保护措施等。

a） 收集图片信息目的要求：应与业务功能场景相关，不应仅以改善服务质量、提升使用体验、研发新产品、增强安全性等为由强制个人信息主体同意收集跟场景无关的图片信息。

b） 收集图片信息的方式要求：移动应用软件通过读取媒体库等方式收集图片信息时，应征得个人信息主体对相应权限的授权同意；移动应用软件通过相机/屏幕截图生成图片信息时，应为个人信息主体呈现显性的拍摄界面/屏幕截图界面。

c） 收集图片信息的范围要求：当个人信息主体仅选取一张或几张图片时，非个人信息主体主动触发（如预览），不应读取图片库中其他图片信息。

d） 收集图片信息的频率要求：如不是个人信息主体主动发起或授权同意 APP 读取图片库，APP 应限定满足业务目的的最低收集频率。

APP不同场景下最小必要收集图片信息如表2：

表 2　APP 不同场景下最小必要收集的图片信息

场景	图片基本信息	图片附加信息	图片位置信息
社交	是	可选	可选
媒体发布	是	可选	可选
图片加工	是	可选	可选
图像识别	是	可选	可选
云盘备份	是	是	是
客服/售后	是	可选	可选
注：表格中“可选”是指App可单独获得“图片附加信息”和“图片位置信息”的授权同意，收集“附加信息”和“位置信息”，或者可根据自身能力选择把图片作为整体向个人信息主体申请授权同意并收集图片信息。			

8.3　存储阶段

8.3.1　本地存储

APP本地存储图片信息应满足以下要求：

a） 应在安全策略控制范围内，保证只有个人信息主体具有所存储图片信息的读、写、修改和删除的权利。（图片自动压缩可改变图片信息的除外）。

b） 在使用个人生物识别信息用于身份识别、认证等功能时，在实现身份鉴别等功能后应删除可提取个人生物识别信息的原始图片（如指纹、人脸识别、掌纹、虹膜等），应加密且仅存储个人生物识别信息的特征信息，并与个人身份信息分开存储。

移动应用软件存储期限应按业务实现功能所需最短时限，法律法规要求的除外。

8.3.2　云存储

APP本地存储图片信息应满足以下要求：

a） 应对所存储图片信息数据进行访问控制，包括但不限于身份认证和鉴别等机制。宜对云端个人信息主体图片提供加密存储功能。

b） 使用个人生物识别信息用于身份鉴别功能时，若需上传包含生物特征识别信息的图片（如指纹、面部、掌纹、虹膜等）到云端处理时，应征得个人信息主体单独同意，且采用显著方式（如图标闪烁、状态栏提示、自定义提示条等）提示个人信息主体。

c） 如有云端自动备份照片功能，宜向个人信息主体告知备份的时机、频率等，以及提供停止自动备份的功能。若需在云端图片识别，宜告知收集图片识别信息的目的、范围、方式、频率，并征得个人信息主体授权同意。

8.4 使用阶段

8.4.1 图片信息展示限制

APP展示图片信息时，个人信息控制者宜对展示的个人信息采取去标识化处理等措施，降低个人信息在展示环节的泄露风险。在不同场景下的图片展示规范如表3：

表 3 不同场景下图片信息展示规范

场景	展示图片规范
社交	展示时宜给个人信息主体提示图片中是否含图片附加信息和图片位置信息并允许个人信息主体选择删除
媒体发布	展示时宜给个人信息主体提示图片中是否含图片附加信息和图片位置信息并允许个人信息主体选择删除
图片加工	展示时宜给个人信息主体提示图片中是否含图片附加信息和图片位置信息并允许个人信息主体选择删除
图像识别	图像识别后的信息展示给个人信息主体时，可对其中个人敏感信息采取去标识化处理
云盘备份	展示时宜给个人信息主体提示图片中是否含图片附加信息和图片位置信息
客服/售后	未经个人信息主体同意，不应对第三方展示

8.4.2 图片信息使用目的的限制

使用图片信息时，APP不应超出与收集时所声称的目的具有直接或合理关联的范围。如因业务需要，确需超出上述范围使用个人信息的，应再次征得个人信息主体明示同意。

8.4.3 图片信息汇聚融合

APP对图片信息和收集的其他个人信息汇聚融合，应遵循使用目的的限制要求，并开展个人信息安全影响评估，采取有效的个人信息保护措施。

8.4.4 图像识别限定

应用设计或开发者不应对图片信息采取隐蔽手段挖掘和分析归纳个人信息主体的身份特征数据。

未经个人信息主体单独同意，不应将收集的图片信息用于识别身份。

8.5 删除阶段

对收集、加工、传输阶段所使用的缓存图片信息，应用应为个人信息主体提供自动删除或手动删除的功能。未经个人信息主体单独同意，不应删除非本应用存储目录下的图片原始二进制码。

9 评估流程和方法

9.1 评估流程

APP收集使用图片信息最小必要的评估流程应遵循YD/T xxxx-xxxx《移动互联网应用程序（APP）收集使用个人信息最小必要评估规范 第1部分：总则》中的评估流程。评估方根据被评估方提供的技术说明文档、被评估APP样品等材料，确定APP的个人信息处理活动中涉及的个人信息类型包括图片信息时，可以依据本评估规范进行评估。

9.2 评估方法

9.2.1 权限授权的评估方法

测试编号：9.2.1
测试项目：图片信息的权限授权最小必要评估
测试要求：见本文件 8.1
预置条件：被评估 APP 处于正常状态
测试步骤： a） 通过访谈或审查文档等方式检查 APP 权限授权的内容，判定其是否涉及图片生成或使用的功能； b） 运行 APP，在 APP 首次使用前，是否获得了个人信息主体的权限授权； c） 运行 APP，对照表 1，APP 是否在需要用到位置信息时，才向个人信息主体征得权限授权。
预期结果：若以上测试步骤结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

9.2.2 收集阶段评估方法

测评编号：9.2.2
测评项目：图片信息在收集阶段的最小必要评估
项目要求：8.2
预置条件：被评估 APP 处于正常状态
测评步骤： a） 运行 APP，检查 APP 在收集个人图片信息前，是否以显著方式、清晰易懂的语言真实、准确完整的向个人信息主体告知了收集图片信息的目的、方式和范围； b） 通过访谈或审查文档等方式检查 APP 收集图片信息的信息类型，判断信息类型是否在可收集范围内。若应用场景不属于典型场景或超过可收集信息类型，则通过访谈等方式评估收集信息是否必要； c） 分别检查 APP 是否满足 8.1.1 中 a、b、c 条中收集图片信息目的、方式、范围的要求； d） 检查 APP 是否满足 8.1.1 中 d）条中收集图片信息频率的要求。
预期结果： a） 在步骤 1 后，若以上测试步骤结果为肯定，则步骤 1 判定为未见异常，否则判定为不符合要求，该项测评结束； b） 在步骤 2 后，若测试步骤为肯定，则步骤 2 判定为未见异常，否则判定为不符要求，该项测评结束； c） 在步骤 3 后，若测试步骤为肯定，则步骤 3 判定为未见异常，否则判定为不符合要求； d） 在步骤 4 后，若测试步骤为肯定，则步骤 4 判定为未见异常。

9.2.3 存储阶段评估方法

测试编号：9.2.3.1
测试项目：图片信息在本地存储阶段的最小必要评估
测试要求：见本文件 8.3.1
预置条件：被评估 APP 处于正常状态
测试步骤： a） 通过访谈或审查文档等方式检查 APP 对图片信息在端侧的本地存储，是否满足 8.3.1

的要求； b） 通过功能验证检查非个人信息主体是否可读、写、修改和删除所存储的图片信息； c） 通过功能验证或技术检测检查个人生物识别信息的原始图片在实现身份鉴别等功能后是否删除；通过审查文档和技术检测的方式检查是否仅加密存储了个人生物识别信息的特征信息，是否与个人身份信息分开存储； d） 通过审查文档检查图片在本地存储期限是否符合法律法规的要求，是否超过业务实现功能所需最短时限。
预期结果：若以上测试步骤结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

测试编号：9.2.3.2
测试项目：图片信息在云存储阶段的最小必要评估
测试要求：见本文件 8.3.2
预置条件：被评估 APP 处于正常状态
测试步骤： a） 通过功能验证检查APP对图片信息的云端存储是否提供身份认证和鉴别等访问控制措施，通过访谈或审查文档等方式检查云端个人信息主体图片是否加密存储； b） 通过功能验证检查云端使用个人生物识别信息进行身份鉴别时，是否征得个人信息主体单独同意，是否采用显著方式（如图标闪烁、状态栏提示、自定义提示条等）提示个人信息主体； c） 通过审查文档检查云端自动备份是否向个人信息主体告知备份的时机、频率等，通过功能验证检查是否提供停止自动备份的功能； d） 通过审查文档检查在云端图片识别场景是否告知收集图片识别信息的目的、范围、方式、频率，通过功能验证检查云端图片识别场景是否征得个人信息主体授权同意。
预期结果：若以上测试步骤结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

9.2.4 使用阶段评估方法

测试编号：9.2.4.1
测试项目：图片信息的展示限制的最小必要评估
测试要求：见本文件 8.4.1
预置条件：被评估 APP 处于正常状态
测试步骤： a） 通过功能验证检查 APP 在社交、媒体发布、图片加工、图片识别、云盘备份场景下图片信息的展示是否满足表 3 的要求；通过访谈或审查文档检查在客服/售后场景对第三方展示个人信息主体图片是否经过个人信息主体同意。
预期结果：若以上测试步骤结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

测试编号：9.2.4.2
测试项目：图片信息的使用目的的限制的最小必要评估
测试要求：见本文件 8.4.2

预置条件：被评估 APP 处于正常状态
测试步骤： a） 通过访谈或审查文档等方式检查APP声称的目的和其实际收集和使用个人信息的目的是否相符； b） 通过访谈或功能验证检查超范围使用个人信息时是否再次征得个人信息主体明示同意。
预期结果：若以上测试步骤结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

测试编号：9.2.4.3
测试项目：图片信息的汇聚融合的最小必要评估
测试要求：见本文件 8.4.3
预置条件：被评估 APP 处于正常状态
测试步骤： a） 通过访谈或审查文档等方式检查APP是否在其声称的目的范围内对图片信息与其他个人信息汇聚融合；通过审查文档检查 APP 是否在个人信息汇聚融合前开展个人信息安全影响评估，以及是否采取有效的个人信息保护措施。
预期结果：若以上测试步骤结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

测试编号：9.2.4.4
测试项目：图片信息中图像识别的限定的最小必要评估
测试要求：见本文件 8.4.4
预置条件：被评估 APP 处于正常状态
测试步骤： a） 通过访谈检查应用设计或开发者是否对图片信息采取隐蔽手段挖掘和分析归纳个人信息主体的身份特征数据； b） 通过访谈和审查文档等方式检查APP是否将收集的图片信息用于对个人信息主体进行身份标识和识别； c） 通过功能验证检查将收集的图片信息用于身份的标识和识别的场景是否经过个人信息主体的单独同意。
预期结果：若以上测试步骤结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

9.2.5 删除阶段评估方法

测试编号：9.2.5
测试项目：图片信息的在删除阶段的最小必要评估
测试要求：见本文件 8.5
预置条件：被评估 APP 处于正常状态
测试步骤： a） 通过功能验证检查 APP 在收集、加工、传输阶段所使用的缓存图片信息，是否可供个人信息主体自动删除或收到删除；通过技术检测检查是否存在未经个人信息主体同意

删除非本应用存储目录下的图片原始二进制码的情形。
预期结果：若以上测试步骤结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

电信终端产业协会团体标准

APP 收集使用个人信息最小必要评估规范 第 3 部分：图片信息

T/TAF 077.3-XXXX

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn