隐私合规检测报告

1、检测APP基础信息

APP名称	全来电
版本号	2.73.84
文件大小	32.55 MB
包名	uni.UNIECAFA94
文件MD5	205CCF03042BAA099CB93A7F94EE51AB
签名证书	CN=qld, OU=全来电科技, O=全来电科技, L=北京, ST=北京, C=CN,CN=qld, OU=全来电科技, O=全来电科技, L=北京, ST=北京, C=CN
minSdkVersion	19
targetSdkVersion	28
是否加固	未加固
评估单位	腾讯应用宝、腾讯安全大数据实验室联合评估
评估时间	2024年05月23日14时35分35秒
检测时长	50分21秒
测试手机操作系统版本	Android8.1

2、检测依据

1、全国人大常委会《中华人民共和国网络安全法》
2、全国人大常委会《个人信息保护法》
3、全国信息安全标准化技术委员会《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》
4、全国信息安全标准化技术委员会《移动互联网应用程序（APP）系统权限申请使用指南》
5、APP专项治理工作组《App申请安卓系统权限机制分析与建议》
6、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》（工信部信管函〔2020〕164号）
7、四部委《App违法违规收集使用个人信息行为认定方法》（国信办秘字〔2019〕191号）

3、检测整体结论

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（工信部信管函〔2020〕164号）

测评结论： 存在风险

风险数量： 2 （共28项检测）

4、检测详情

4.1、 违规收集个人信息 存在2 处风险

场景1 APP未见向用户明示个人信息收集使用的目的、方式和范围，未经用户同意，存在收集IMEI、设备MAC地址和软件安装列表、通讯录和短信的行为。

检测结论 暂无风险

场景2 APP以隐私政策弹窗的形式向用户明示收集使用规则，未经用户同意，存在收集IMEI、设备MAC地址和软件安装列表、通讯录和短信的行为。

检测结论 暂无风险

场景3 APP以隐私政策弹窗的形式向用户明示收集使用规则，但未见清晰明示APP收集设备MAC地址、软件安装列表等的目的方式范围，用户同意隐私政策后，存在收集设备MAC地址、软件安装列表的行为。

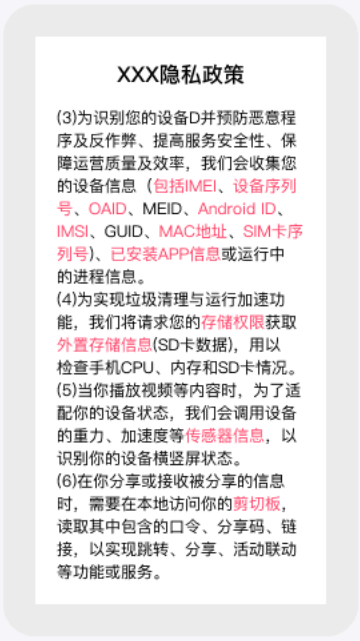
检测结论 存在风险

违规点解析 检测APP在实际运行过程中，收集用户个人信息未在隐私政策中进行相关说明。

整改建议

1.APP或SDK收集个人信息相关行为明确补充在隐私政策协议中；
2.如是SDK收集的个人信息，请您务必在隐私协议中准确写明SDK的名称和对应收集的个人信息。
3.检查具体信息是否写正确。例如检测到收集设备序列号，您只写了设备硬件信息。

请您参考下图示例，将实际检测出未明示行为在隐私政策中补齐



XXX隐私政策

(3)为识别您的设备D并预防恶意程序及反作弊、提高服务安全性、保障运营质量及效率，我们会收集您的设备信息（包括IMEI、设备序列号、OAID、MEID、Android ID、IMSI、GUID、MAC地址、SIM卡序列号）、已安装APP信息或运行中的进程信息。
(4)为实现垃圾清理与运行加速功能，我们将请求您的存储权限获取外置存储信息(SD卡数据)，用以检查手机CPU、内存和SD卡情况。
(5)当你播放视频等内容时，为了适配你的设备状态，我们会调用设备的重力、加速度等传感器信息，以识别你的设备横竖屏状态。
(6)在你分享或接收被分享的信息时，需要在本地访问你的剪切板，读取其中包含的口令、分享码、链接，以实现跳转、分享、活动联动等功能或服务。

行为详情

场景4 APP未见向用户明示SDK收集使用个人信息的目的、方式和范围，未经用户同意，SDK存在收集IMEI、设备MAC地址和软件安装列表、通讯录和短信的行为。

检测结论 暂无风险

场景5 APP向用户明示SDK的收集使用规则，未经用户同意，SDK存在收集IMEI、设备MAC地址和软件安装列表、通讯录和短信的行为。

检测结论 暂无风险

场景6 APP向用户明示SDK的收集使用规则，但未见清晰明示SDK收集设备MAC地址、软件安装列表等的目的方式范围，用户同意隐私政策后，SDK存在收集设备MAC地址、软件安装列表的行为。

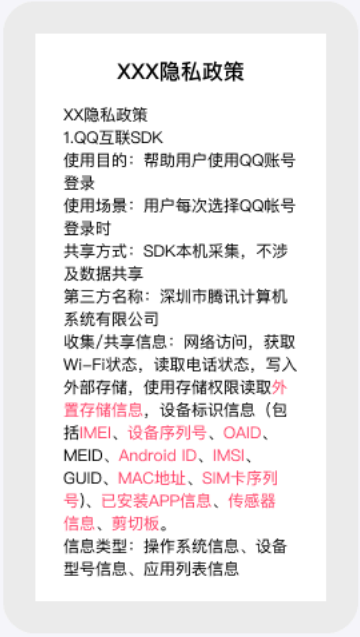
检测结论 存在风险

违规点解析 检测APP在实际运行过程中，收集用户个人信息未在隐私政策中进行相关说明。

整改建议

1.APP或SDK收集个人信息相关行为明确补充在隐私政策协议中；
2.如是SDK收集的个人信息，请您务必在隐私协议中准确写明SDK的名称和对应收集的个人信息。
3.检查具体信息是否写正确。例如检测到收集设备序列号，您只写了设备硬件信息。

请您参考下图示例，将实际检测出未明示行为在隐私政策中补齐


XXX隐私政策

XX隐私政策
1.QQ互联SDK
使用目的：帮助用户使用QQ账号登录
使用场景：用户每次选择QQ帐号登录时
共享方式：SDK本机采集，不涉及数据共享
第三方名称：深圳市腾讯计算机系统有限公司
收集/共享信息：网络访问，获取Wi-Fi状态，读取电话状态，写入外部存储，使用存储权限读取外置存储信息，设备标识信息（包括IMEI、设备序列号、OAID、MEID、Android ID、IMSI、GUID、MAC地址、SIM卡序列号）、已安装APP信息、传感器信息、剪切板。
信息类型：操作系统信息、设备型号信息、应用列表信息

行为详情

场景7 App在征求用户同意环节，未提供明确的同意或拒绝按钮，或者使用“好的”“我知道了”等词语。

检测结论 暂无风险

场景8 App在征求用户同意环节，设置为默认勾选。

检测结论 暂无风险

4.2、 超范围收集个人信息 暂无风险

场景1 APP未见向用户告知且未经用户同意，在YYY功能中，存在收集通讯录、短信、通话记录、相机等信息的行为，非服务所必需且无合理应用场景，超出与收集个人信息时所声称的目的具有直接或合理关联的范围。

检测结论 暂无风险

场景2 APP在运行时，未见向用户告知且未经用户同意，存在每30s读取一次位置信息，非服务所必需且无合理应用场景，超出实现产品或服务的业务功能所必需的最低频率。

检测结论 暂无风险

场景3 APP未见向用户明示SDK的收集使用规则，未经用户同意，SDK存在收集通讯录、短信、通话记录、相机等信息的行为，非服务所必需且无合理应用场景，超出与收集个人信息时所声称的目的具有直接或合理关联的范围。

检测结论 暂无风险

场景4 APP未见向用户明示SDK的收集使用规则，未经用户同意，SDK存在每30s读取一次位置信息，非服务所必需且无合理应用场景，超出实现产品或服务的业务功能所必需的最低频率。

检测结论 暂无风险

场景5 APP未见向用户告知且未经用户同意，在静默状态下或在后台运行时，存在收集通讯录、短信、通话记录、相机等个人信息的行为，非服务所必需且无合理应用场景，超出与收集个人信息时所声称的目的具有直接或合理关联的范围。

检测结论 暂无风险

场景6 APP未见向用户告知且未经用户同意，在静默状态下或在后台运行时，存在按照一定频次收集位置信息、IMEI、通讯录、短信、图片等信息的行为，非服务所必需且无合理应用场景，超出与收集个人信息时所声称的目的具有直接或合理关联的范围。

检测结论 暂无风险

场景7 APP未向用户明示SDK的收集使用规则，未经用户同意，SDK在静默状态下或在后台运行时，存在收集通讯录、短信、通话记录、相机等信息的行为，非服务所必需且无合理应用场景，超出与收集个人信息时所声称的目的具有直接或合理关联的范围。

检测结论 暂无风险

场景8 APP未向用户明示SDK的收集使用规则，未经用户同意，SDK在静默状态下或在后台运行时，存在按照一定频次收集位置信息、IMEI、通讯录、短信、图片等信息的行为，非服务所必需且无合理应用场景，超出与收集个人信息时所声称的目的具有直接或合理关联的范围。

检测结论 暂无风险

4.3、 违规使用个人信息 暂无风险

场景1 APP未见向用户告知且未经用户同意，存在将IMEI/设备MAC地址/软件安装列表等个人信息发送给友盟/极光/个推等第三方SDK的行为。

检测结论 暂无风险

场景2 APP未见向用户明示分享的第三方名称、目的及个人信息类型，用户同意隐私政策后，存在将IMEI/设备MAC地址/软件安装列表等个人信息发送给友盟/极光/个推等第三方SDK的行为。

检测结论 暂无风险

4.4、 APP强制、频繁、过度索取权限 暂无风险

场景1 APP首次启动时，向用户索取电话、通讯录、定位、短信、录音、相机、存储、日历等权限，用户拒绝授权后，应用退出或关闭（应用陷入弹窗循环，无法正常使用）。

检测结论 暂无风险

场景2 APP运行时，未向用户告知XXX权限的目的，向用户索取当前服务场景未使用到的通讯录、定位、短信、录音、相机、日历等权限，且用户拒绝授权后，应用退出或关闭相关功能，无法正常使用。

检测结论 暂无风险

场景3 用户注册登录时，APP向用户索取电话/通讯录/定位/短信/录音/相机/存储/日历等权限，用户拒绝授权后，应用无法正常注册或登录。

检测结论 暂无风险

场景4 APP运行时，向用户索取当前服务场景未使用到的电话/通讯录/定位/短信/录音/相机/存储/日历等权限，且用户拒绝授权后，应用退出或关闭（应用陷入弹窗循环，无法正常使用）。

检测结论 暂无风险

场景5 APP运行时，在用户明确拒绝通讯录/定位/短信/录音/相机/XXX等权限申请后，仍向用户频繁弹窗申请开启与当前服务场景无关的权限，影响用户正常使用。

检测结论 暂无风险

场景6 APP在用户明确拒绝通讯录/定位/短信/录音/相机/XXX等权限申请后，重新运行时，仍向用户弹窗申请开启与当前服务场景无关的权限，影响用户正常使用。

检测结论 暂无风险

场景7 APP首次打开（或其他时机），未见使用权限对应的相关产品或服务时，提前向用户弹窗申请开启通讯录/定位/短信/录音/相机/XXX等权限。

检测结论 暂无风险

4.5、 APP频繁自启动和关联启动 暂无风险

场景1 APP未向用户明示未经用户同意，且无合理的使用场景，存在频繁自启动或关联启动的行为。

检测结论 暂无风险

场景2 APP虽然有向用户明示并经用户同意环节，但频繁自启动或关联启动发生在用户同意前。

检测结论 暂无风险

场景3 APP非服务所必需或无合理应用场景，超范围频繁自启动或关联启动第三方APP。

检测结论 暂无风险

5、集成SDK数量

SDK集成的数量（个）	1
用户“同意”前收集用户信息的数量（个）	0
收集用户信息没有在隐私政策中清晰明示的数量（个）	1

存在风险的SDK详情

其他SDK详情