2018

移动金融用户个人信息安全

测评报告

南都个人信息保护研究中心

联合发布方：

南都个人信息保护研究中心　　中国人民大学金融科技与互联网安全研究中心

法律顾问：北京玺泽律师事务所

目录

前言

有学者认为，2018 年是公众个人信息保护意识觉醒的元年。从支付宝年度账单事件，到江苏消保委诉百度侵犯用户隐私；从李书福称微信的聊天内容可能被腾讯窥视，到今日头条的算法受到用户的质疑。一系列舆论热点的集中爆发，无疑预示着公众在互联网时代的隐私保护意识已经全面觉醒。

然而，我们通过长期的观察与测评发现，互联网企业对用户隐私保护的重视程度却普遍不高，未能跟上用户隐私保护意识的发展。

以移动端 APP 为例，在谷歌 Play、苹果 App Store 上，均有要求凡涉及个人信息及敏感信息的网络运营商必须提供隐私政策，说明如何收集使用、分享和处理用户数据。但并非所有上线的 APP 都有隐私政策。在大多数无这方面要求的应用商店里，情况更是如此。

2017 年 12 月，南都个人信息保护研究中心推出《2017 个人信息保护年度报告》，就十多个行业共 1550 个网站和 APP 的隐私政策进行测评，结果发现，平台隐私政策透明度的分布都是陡峭的金字塔型，即透明度高的极少，透明度低则占到绝大多数，超过总数的 80%，更有 17 家应用根本没有隐私保护协议或政策。

上述报告还发现，金融类互联网应用在测评中的表现不佳，成绩排在旅游类、求职类、交友类应用之后，隐私政策透明度低的金融类 APP 占比甚至高于 90%。这一报告一经发布，引起广泛讨论。

随着互联网金融的迅速发展，有越来越多用户的个人信息在各类金融平台聚集，其中大部分是与个人财产相关的敏感信息。令人担忧的是，个人数据的泄露也日益严重，给消费者造成经济损失。

从企业自身发展的角度看，近几年的个人信息泄漏案例通常都是突发的、大规模且后果非常严重的，对企业的声誉、品牌形象和经营绩效造成很大的负面影响。尤其是在大数据时代，流动的数据创造价值，数据开放利用将是趋势，这需要企业建立保护个人信息的可信任形象。

如何更好的保护消费者权益，如何解决日益增多的权益需求与目前我国个人信息权益保护相关法律有限的困境，是本次测评报告中要讨论的问题。

二、测评方法

（一）测评对象

本次测试针对移动金融交互类 APP（应用程序）。

所谓移动金融，是指以移动互联网为基础，以移动智能终端为载体，向用户提供的随时随地随身的金融服务。交互类的判断依据是，APP 是否需要用户注册，是否需要用户提供信息。

基于以上定义，本次测评根据产品所提供的服务与人们生活的相关度，用户使用量和使用频率等因素，选择了公众使用最为频繁的 200 款移动金融交互类 APP 产品。其中大致包括四类：借贷类 APP、理财类 APP、支付类 APP 与实体银行的线上产品。

（二）样本采集

（1）采集设备

本次测评采集设备主要为安卓移动端与 IOS 移动端，测评的第一部分与第三部分考察 IOS 系统的产品，第二部分则考察安卓系统产品。IOS 移动端主要使用苹果手机在 App Store 安装时 APP 的版本信息进行采集。安卓移动端则是在安卓手机上自带的应用市场或下载的”应用宝“等应用市场进行采集。

（2）测评时间

本次测评的第一及第三部分测评取证采集时间为 2018 年 2 月 1 日至 2 月 4 日；第二部分测评取证采集时间为 2018 年 2 月 17 日至 2 月 20 日，先后采取自评、交换互评的方式，对评分较高或较低的样本以及随机抽取的样本进行反复核实。在上述取证时间之外的修改不计入本次测评结果。

（3）采集内容

视频资料：为了便于后期核查，使用摄像机、屏幕录像专家软件等对整个采样取证过程进行全程录像。

图片资料：对隐私政策、敏感信息收集页进行截图。

文本资料：对采集的《隐私协议》等相关文件全文复制，建立独立的 word 文档，以便后期查阅、评分以及作为证据使用。

上述资料统一收集至一个文件夹，按行业编号整理。

（三）测评内容与计分

本测试针对一款移动金融交互类 APP 产品共考察三个方面的个人信息保护水平，最终汇总得到测评结果。这三方面分别是：

（1）：“隐私政策合规”：考察移动金融交互类 APP 产品的“隐私政策”（或“用户协议中的相关部分）文本是否合规。测试标准共包括 13 个方面，对照测评标准，有相关内容加分，无相关内容减分。总分 100 分。

（2）：“敏感权限获取合规”：考察移动金融交互类 APP 产品向系统申请获取用户何种敏感信息权限，是否遵循了《网络安全法》合法、正当、必要性原则与《个人信息安全规范》的最小够用原则。总分 25 分。

（3）：“财产身份信息收集告知合规”：考察移动金融交互类 APP 产品在收集用户财产信息与实名认证身份信息等敏感信息时，是否做到明确告知，并取得用户明示同意。总分 15 分。

（四）法律依据

本次测评依照的，大都是与互联网行业更为密切的法律法规，如《中华人民共和国网络安全法》、《中华人民共和国消费者权益保护法》、《网络交易管理办法》、《电信和互联网用户个人信息保护规定》、《互联网电子邮件服务管理办法》、《移动互联网应用程序信息服务管理规定》、《计算机信息网络国际联网管理暂行规定实施办法》、最高人民法院《关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》等十余部法律法规及相关法律文件，同时也参考了《信息安全技术公共及商用服务信息系统个人信息保护指南（GB/Z 28828-2012）》、《中国互联网定向广告用户信息保护行业框架标准》等。

将于 2018 年 5 月 1 日正式施行的国家标准 GB/T 35273-2017 《信息安全技术 个人信息安全规范》是本次测评参照最多的法律文件，特别是其中对于个人信息与敏感信息的界定，对于信息收集的明示同意与最少够用原则的定义，都在本次测评中得以体现。

需要强调的是，《信息安全技术 个人信息安全规范》并非具有强制力的法律法规，本次测评所采用的标准也只代表第三方机构的观点，只提供更合规的建议，企业并非必须按照这一标准行事。但可以通过企业主动合规与执法部门参照执法等形式具备约束力。

三、测评及结果

（一）“隐私政策合规”

（1）定义

“隐私政策”，是企业与用户之间关于如何处理和保护用户个人信息的基本的权利义务的文件，用以告知用户个人信息如何被收集、使用、与第三方共享的情况。通常在用户首次注册时在页面上展示。它不仅是对企业的束缚，也是企业提示用户自主、自愿、合理提供和处理个人信息，并区分与用户责任的依据。因此，此部分测评考察的即是测评对象的“隐私政策”文本是否合规。

不同于美国大部分网站单独制定个人信息保护政策，并统一命名为具有较高识别度、便于用户发现的“隐私政策”（Privacy policy）或“隐私声明”（privacy statement），国内的互联网企业关于隐私保护的命名较为混乱，有称“隐私（权）政策”、也有称“隐私权声明”、“隐私权策略”、“隐私保护条例”等。同时，更多企业的个人信息保护规定散见于“用户协议”、“使用条款”甚至是“免责声明”中，所以在企业公开的相关协议中，凡有个人信息保护说明并处于隐私政策涵盖范围内的，原则上均可参与测评。

（2）依据法律法规条文

《中华人民共和国网络安全法》第二十二条：网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

《电信和互联网用户个人信息保护规定》第八条：电信业务经营者、互联网信息服务提供者应当制定用户个人信息收集、使用规则，并在其经营或者服务场所、网站等予以公布。

《电信和互联网用户个人信息保护规定》第九条：未经用户同意，电信业务经营者、互联网信息服务提供者不得收集、使用用户个人信息。电信业务经营者、互联网信息服务提供者收集、使用用户个人信息的，应当明确告知用户收集、使用信息的目的、方式和范围，查询、更正信息的渠道以及拒绝提供信息的后果等事项。电信业务经营者、互联网信息服务提供者不得收集其提供服务所必需以外的用户个人信息或者将信息用于提供服务之外的目的，不得以欺骗、误导或者强迫等方式或者违反法律、行政法规以及双方的约定收集、使用信息。电信业务经营者、互联网信息服务提供者在用户终止使用电信服务或者互联网信息服务后，应当停止对用户个人信息的收集和使用，并为用户提供注销号码或者账号的服务。

（3）测评标准

在深入研究了国内相关的法律法规、行业标准、业界十几家完善的“隐私政策”实例以及国外的相关法律规定后，由测评方反复修改制定隐私政策的测评标准。

为了保证标准的严谨性，我们还专门就测评标准征询了专家小组成员的意见，力求在架构设计、条款描述、内容等方面尽可能客观、全面、可操作。

隐私政策测评标准十三大项分别如下：

1. 是否提供了个人信息保护政策；

2. 个人信息保护政策的规范性；

3. 履行必要的告知和警示义务；

4. 用户选择和同意权；

5. 用户的访问、更正及删除权；

6. 向第三方披露用户个人信息；

7. 安全承诺；

8. 使用个人信息向用户发送商业资讯；

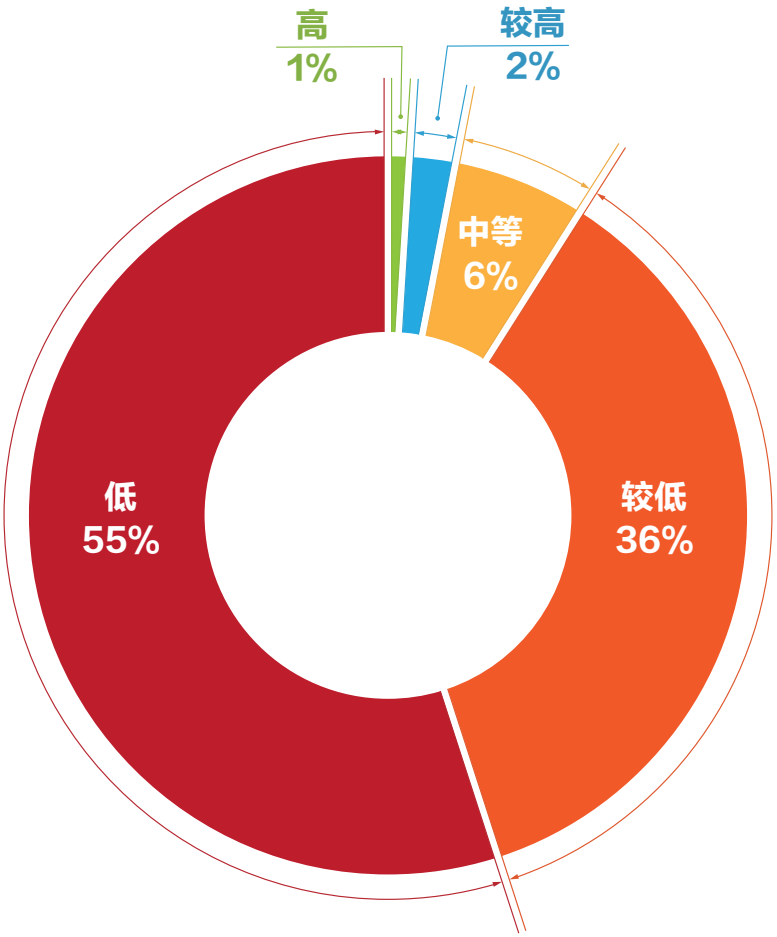
9. 特殊情形下个人信息的处理原则；

10. 对个人信息保护政策进行修改的原则；

11. 有关的救济措施；

12. 对于使用 Cookie、clickstream 和 web beacon 等技术的专门声明；

13. 对链接第三方网站的免责说明。



【图 1. 200 款移动金融交互类 APP 产品隐私政策合规程度百分比】

a. 总体情况

按照总分，200 款 APP 可划分为五个层级，分别为合规程度高（90 分以上）、合规程度较高（76-90 分）、合规程度中等（61-75 分）、合规程度较低（41-60 分）、合规程度低（40 分及以下）。由图一可以看到，基于我们的测评标准，200 个平台中仅有 2 个能够达到隐私政策合规程度高的标准，合规程度较高的也只有 3 个平台，高与较高的 APP 一共只占总数的 3%；透明度中等的平台个数为 13 个，占比 6%；而透明度较低和透明度低的平台个数相加则多达 182 个，超过总数的 90%。

b. 红榜与黑榜

红榜	
APP	总分
支付宝	95
京东金融	95
人人贷	82
小米金融	82
平安普惠	80

在合规程度最高的几款 APP 中，支付宝、京东金融评分并列第一，评分为 95 分；人人贷、小米金融并列第三，评分为 82 分。值得注意的是，阿里巴巴与京东的产品都参与了 2017 年 8 月由中央网信办等四部委发起的联合测评，因此，支付宝与京东金融在此次参与测评的产品中名列前茅，并且成绩超过其他 APP 10 分以上。

黑榜	
APP	总分
来存吧票据理财 – 金融投资平台	0
短融网	0
趣店	0
隆金宝	0
中兴财富	0
珠宝贷	0
宜贷网	0
聚车金融	0
易港金融	0
诚汇通	0
三信理财	0
钱内助	0
E 都市钱包	0
渝金所	0
精融汇	0
绿化贷	0
中潮金服	0
58 车贷	0
中国银行	0
中国建设银行	0

在透明度低的 111 款 APP 中，有 20 款因为完全没有隐私政策得到 0 分。这意味着，这些会收集用户实名信息、银行卡信息、信用信息等敏感信息的 APP，根本没有任何保护用户个人信息的承诺文本，保护隐私意识淡薄，用户面临着信息被不当泄露等风险，应对这些 APP 保持警惕。

需要特别提醒的是，用户协议或隐私政策应该在用户注册前就在页面提示，而不是注册之后。这样才能保证用户在使用产品前就对其权利义务充分知晓。

黑榜中需要注意的是，中国银行与中国建设银行由于是实体银行的线上应用平台，与其他 APP 在用户协议签订时略有不同。一般情况下，银行 APP 的用户往往已经在线下柜台完成面对面签约再使用线上平台。因此有观点认为，实体银行的线上产品不需要再提供用户协议与隐私政策。但本报告认为，线上收集个人信息与线下收集个人信息，在收集内容、存放方式、保护手段等都有很大不同，因此实体银行的线上产品应当提供专门的隐私政策。

c. 普遍失分点

由于每款 APP 的隐私政策文本不同，失分点也不尽相同。但有一些条款，接受测评的 APP 普遍都有所缺失。

根据测评结果，200 款 APP 中，有 197 款都未在隐私政策中提及下述相关内容：产品和服务如提供附加功能，需要收集更多的个人信息时，应向个人信息主体逐一说明收集个人信息的必要性，并允许个人信息主体进行选择。当个人信息主体拒绝时，可不提供相应的附加功能，但仍应保证向个人信息主体提供核心业务功能。

这一承诺意在保证对用户个人信息收集的最少够用原则。例如，一款理财类 APP 拥有论坛功能，能够通过收集用户通讯录中的信息添加好友，一起在论坛中讨论发帖。此时，这款 APP 就需要在隐私政策里做出相关声明，告知用户读取通讯录的用途和必要性，并且告知用户即使不同意收集通讯录信息也并不影响这款 APP 的理财功能使用。

测评显示，只有 3 款 APP 在隐私政策中包括了上述内容。例如，支付宝在隐私政策中写道：在您进行指纹支付时，需要使用您的指纹信息进行验证……如您不想提供指纹信息，仍可通过输入密码方式进行支付。

此外，有 196 款 APP 未在隐私政策中说明，产品和服务停止运营时，处理用户个人信息的方式。如：及时停止继续收集个人信息；以逐一送达或网站公告的形式通知用户停止运营的情况；将删除用户个人信息等；而《电信和互联网用户个人信息保护规定》明确规定，电信业务经营者、互联网信息服务提供者在用户终止使用电信服务或者互联网信息服务后，应当停止对用户个人信息的收集和使用，并为用户提供注销号码或者账号的服务。因此，本报告认为，APP 需要在隐私政策中提及上述内容。

有 193 款未在隐私政策中明确界定“个人信息”，“非个人信息”，“个人敏感信息”等定义，而这一点对考察一款 APP 是否针对用户的个人敏感信息使用更加妥善至关重要。

有 194 款 APP 未在隐私政策中提及给予用户退订或拒绝的权利，并提供有效途径及操作指引。大多数隐私政策在描述中都明确提出，一旦用户勾选同意《用户服务协议》或《隐私政策》从而注册成功，就表示“用户同意接受本公司通过短信、电子邮件或其他方式向用户发送商品促销或其他相关商业信息”，而只字不提用户拥有拒绝和退订的权利，或是退订的操作方法。

177 款 APP 未向用户提供查询、更正、补充或删除的有效途径及操作说明。《中华人民共和国网络安全法》第四十三条规定：个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。今年 1 月，工信部也曾要求，电信业务经营者、互联网信息服务提供者在用户终止使用电信服务或者互联网信息服务后，应当停止对用户个人信息的收集和使用，并为用户提供注销号码或账号的服务。因此 APP 也应在隐私政策中做出

相关承诺。

通过对 200 款 APP 的隐私政策进行测评后我们还发现，大多数应用的隐私条款都包括以下 3 条：1、平台可以将你的信息分享给第三方；2、平台可以利用你的个人资料进行推广、促销等工作；3、平台会根据行业标准惯例保护你的个人资料，但鉴于技术限制，不能确保不会泄露。

众所周知，披露个人信息是有风险的，因为没有任何一个企业能保证数据 100% 安全。然而，针对发生或可能发生个人信息泄漏、毁损、丢失的情况，极少数企业明确提出将承担法律责任，并及时通知受影响的用户和采取补救措施。事实上，这些都可以视为企业在削减自己的责任。

上述“霸王条款”在 200 款 APP 的测评过程中屡见不鲜，措辞也极为相似。不难看出，隐私政策普遍存在言语模糊、更新缓慢、暗藏格式条款等弊病。

（5）结论

在接受测评的 200 款移动金融交互类 APP 产品中，仅有 9% 合规程度达到及格，在 60 分以上。其余 91% 的 APP 测评结果都在 60 分以下，合规程度不及格。其中，达到合规程度高的仅有两家，合规程度低的却有 111 个，超过半数。

200 家 APP 中，仅有两家达到 90 分以上，合规程度高；却有 20 家为评分 0 分，即没有隐私政策。

由测评结果来看，移动金融交互类 APP 产品的隐私政策普遍未清晰地区分个人信息与个人敏感信息，对于后者没有特殊的保护承诺。此外，对于核心业务与非核心业务的个人信息收集也未做区分，而是抱着“无论是否需要，一律收集上来再说”的态度对待用户个人信息。

此外，参加测试的 200 家 APP 隐私协议还普遍对于个人信息的分享与披露言语模糊、措辞格式化，推卸企业责任、暗藏霸王条款是普遍现象。

（二）“敏感权限获取合规”

（1）定义

如果说测评的第一部分是考察一款移动金融交互类 APP 产品在保护用户个人信息的**文本与承诺**上是否合规，那么本部分的测试考察的便是在**实际操作**中，一款 APP 在收集用户信息中的合规问题。

一款 APP 在收集用户个人信息时，除了用户主动填写个人信息外，还会通过向系统申请权限的方式，让机器收集用户个人信息，如申请读取用户通讯录的权限，以收集通讯录中手机号码的信息；又如获取摄像头的权限，以收集用户拍摄的照片信息。

在实际使用中，一款 APP 向系统申请的权限可多达上百条，本次测评特别将这些权限中的“敏感权限”（或称“危险权限”，即涉及到个人敏感信息收集的权限）作为考察对象。

本次测评使用了安卓官方目前对于各类权限的分类，认为摄像头、麦克风、手机通讯录、手机短信、传感器（记步工具或手指按压感应等）与地理位置六种权限为敏感权限，在此基础上考察 APP 是否向系统申请了这一权限，申请这一权限可能读取的个人信息是否合法合规。

需要特别指出的是，由于系统的封闭性，这一部分测评未使用苹果手机作为测试工具，而是使用了安卓系统的手机。APP 则从手机自带应用商店与“应用宝”等安卓商店下载。

（2）法律法规相关条文

《中华人民共和国网络安全法》第四十一条：网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息。

《个人信息安全规范》确立“收集个人信息最小化要求”，即收集的个人信息应与实现产品或服务的业务功能有直接关联。直接关联是指没有该信息的参与，产品或服务的功能无法实现。

（3）测评方式

一款 APP，通常有三处可以查询到其获取的权限列表，第一处是应用商店中的简介；第二处是安装应用时（或首次打开时）跳出的权限列表，用户直接可见；第三处是安装包中的 xml 文件，它相当于列明了一款应用“向安卓系统申请允许读取用户哪些权限”。

由于前两处往往由 APP 开发方自己填写设置，或有缺失，而 xml 文件中是最全列表，因此这一部分测试的方式是通过下载安卓商店中相关 APP 的 apk 文件（安装包），解压得到其中的 xml 文件来确定获取的权限。

需要注意的是，xml 文件中的列表虽然不代表这款 APP 一定会读取列表中权限关联的各项隐私，但通俗地说，这像是拿到了打开家门的钥匙。因此，可作为测评的对象。

（4）最小化原则的判别

从 xml 文件中解压出 200 款 APP 获取摄像头、麦克风、手机通讯录、手机短信、地理位置、传感器这六项隐私权限的情况后，需要判断哪些权限没有遵循最小化原则。

在判断一款 APP 获取一项权限是否遵循了最小化原则时，本次测评以《个人信息安全规范》中最小化原则的要求作为主要判断依据，即“收集的个人信息应与实现产品或服务的业务功能有直接关联。直接关联是指没有该信息的参与，产品或服务的功能无法实现。”

（5）测评结果

A. 读取手机短信权限——不符合最小化收集原则

通过多方采访求证，我们了解到读取手机短信权限通常是用来帮助用户自动填写短信验证码，我们判断，这一功能与此次参与测评的 200 家移动金融的业务功能没有直接关联，即使不使用短信读取功能，用户依然能够自己手动填写完成短信验证码的输入，因此这一权限所读取的用户个人信息不符合最小化手机原则。

尽管如此，200 款移动金融交互类 APP 产品中仍有 95 款向系统申请了读取用户短信的功能，几乎达到半数。值得警惕的是，用户的短信内容中常常包含银行卡余额、短信验证码等敏感信息，一旦泄露后果严重，因此收集这一信息的 APP 在此部分测评中扣去了相应的分数。

B. 开启麦克风权限——不符合最小化收集原则

开启麦克风，通常与需要语音输入的功能相关，如行车地图类 APP 中需要语音输入目的地等。但在移动金融交互类 APP 产品中，我们并没有发现哪一项功能需要通过输入语音实现，即使没有开启麦克风，用户仍然能够通过文字输入的方式实现所需功能，所以此项我们仍然认为不符合最小化收集原则。

根据测评结果，有 106 款 APP 读取了这一权限，超过半数。在测评中扣除了相应分数。

C. 读取地理位置的权限——不符合最小化收集原则

读取地理位置的权限，指能够通过 GPS 或 WIFI 获取用户的精确位置。这项权限通常在地图类、打车类 APP 中需要使用。我们考察 200 款移动金融交互类 APP 产品后发现，无论是借贷类、支付类抑或理财类、实体银行的线上产品，都没有功能或服务必须有读取地理位置的权限才能实现。

测评结果显示：200 款 APP 中有 173 款都要求读取地理位置，当我们拒绝 APP 读取这项权限时，对于使用 APP 并未有任何影响，可见，这项权限并非实现某项功能服务所必要，不符合最小化收集原则。

D. 读取传感器的权限——不符合最小化收集原则

手机中的传感器权限，通常是指手机中通过相关元件感知热、光、力、声等信息的权限。如通过传感器获得用户每天行走的步数，获得用户声纹等。目前传感器常在运动类 APP 和登录时使用。

针对移动金融交互类 APP 产品，我们未发现其中有提供声纹或指纹登录功能的，同时也未发现有计步功能。因此，本报告认为，读取传感器的数据也不符合最小化收集原则。

E. 读取手机通讯录权限——不符合最小化收集原则

通常读取手机通信录，都与社交功能相关，如社交交友类软件中，需要读取通讯录来邀请现实中的好友成为 APP 中的好友。

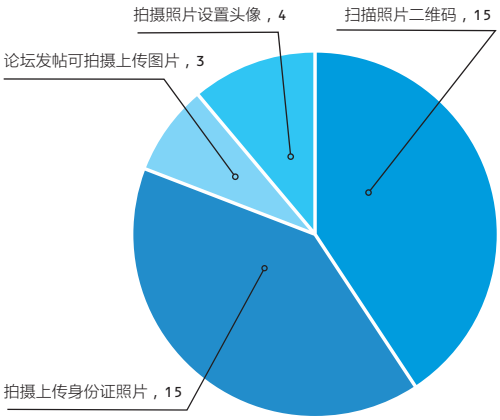
移动金融交互类 APP 产品究竟是否需要社交功能，一直以来存在争议。支付类、理财类 APP 的相关功能并不需要通讯录的信息予以实现，但借贷类 APP 往往会与通讯录产生联系。如现今的一些借贷类 APP 会向通讯录中的好友家人催债等。虽然催债这项功能需要手机通讯录信息的加入才能实现，但目前借贷催债仍处在法律的灰色地带，未经过通讯录上的亲友同意，就打电话催债的行为无疑会对借债人的亲友造成骚扰。在新闻媒体的相关报道中，已经有很多人表示对此不厌其烦。因此，本报告认为，借贷类 APP 不应该读取用户通讯录来作为催债的对象，而应该由借债人主动填写担保人或其认为可以作为催债对象的亲友。

在接受测评的 200 家 APP 中，有 97 款 APP 都获取了读取通讯录的权限，这一行为不符合最小化收集原则，扣除了相应的分数。

F. 读取照相机权限——部分符合最小化收集原则

通过对 200 款移动金融交互类 APP 产品的考察，我们发现读取照相机所获得的个人信息与其中一部分 APP 的功能与服务直接相关，没有照相机的权限，这项功能无法实现。

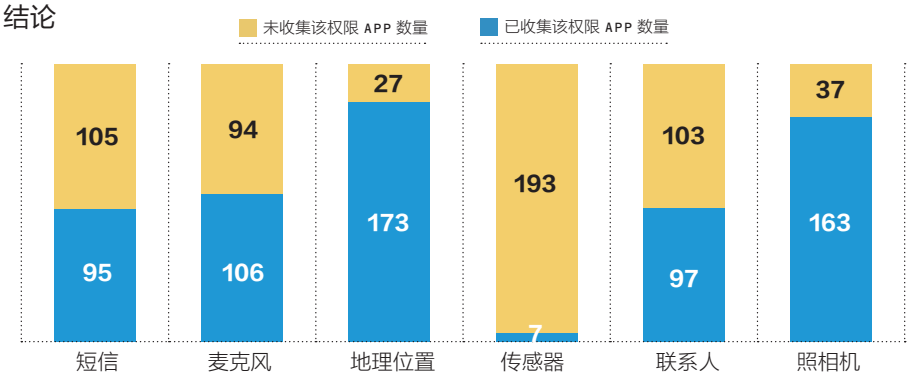
我们将照相机参与的功能分为四种：扫一扫支付、上传身份证照片、论坛发图片帖和拍照更换头像。具有这四种功能的 APP 个数分布如下图：



【图 2. 与照相机相关功能的 APP 个数分布】

在上述四种功能中，有 15 款 APP 拥有扫二维码的功能，由于在支付时，只能通过摄像头扫描实现，因此我们认为上述 15 款 APP 未违反最小化收集原则；在论坛发图片这一功能，如果只能通过发图片才能完成发帖的作用，我们也认为未违反最小化收集原则，这一类 APP 有 3 款；对于拍摄身份证上传功能，我们认为只有那些不能通过手动填写身份证号，而只能通过拍摄上传身份证照片进行实名认证的 APP 才符合最小化收集原则，这样的 APP 有 15 款；同样，拍照上传头像的功能中，如果只能通过拍照上传，才被认为符合最小化收集原则。

（6）结论



【图 3. 获取敏感权限的 APP 数量分布】

对于 APP 通过获取各种手机系统权限收集的个人信息，我们考察了摄像头、麦克风、手机通讯录、手机短信、传感器、地理位置六种敏感权限。我们认为，其中麦克风、手机通讯录、手机短信、传感器、地理位置这五种权限都不能看做移动金融交互类 APP 产品必须要收集的信息，即缺少这些信息，APP 的功能使用不会受到影响。

然而，有 95 款 APP 获取了读取短信的权限；106 款获取了使用麦克风的权限；173 款获取了用户地理位置权限；7 款获取了使用传感器的权限，97 款获取了读取手机通讯录的权限。我们认为上述 APP 的行为都违反了最小化收集原则 ,在这一部分的测评中不能得分。

六种权限中，我们认为支付时的扫一扫、金融论坛发帖、上传身份证与更换头像这几项功能中，都有可能必须要照相机的参与才能实现。共有 163 款 APP 获取了照相机权限，但其中仅有 37 款有相关的功能需要获取照相机权限，遵守了最小化收集原则。因此只有这 37 款 APP 在这一部分的测评中不扣分。

（三）“财产身份信息收集告知合规”

（1）定义

这一部分的测评涉及到移动金融交互类 APP 产品的特色功能，即财产信息与身份信息收集告知的合规情况。此处的财产信息主要指用户的银行卡、房屋等信息，身份信息则包括实名认证需要的身份证信息等。

（2）依据法律法规条文

《中华人民共和国网络安全法》第四十一条：网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

《中华人民共和国消费者权益保护法》第九条:消费者享有自主选择商品或者服务的权利。

《信息安全技术 个人信息安全规范》中规定：收集个人信息前，应向个人信息主体明确告知所提供产品或服务的不同业务功能分别收集的个人信息类型，以及收集、使用个人信息的规则（例如收集和使用个人信息的目的、收集方式和频率、存放地域、存储期限、自身的数据安全能力、对外共享、转让、公开披露的有关情况等），并获得个人信息主体的授权同意；

收集个人敏感信息时，应取得个人信息主体的明示同意。应确保个人信息主体的明示同意是其在完全知情的基础上自愿给出的、具体的、清晰明确的愿望表示；通过主动提供或自动采集方式收集个人敏感信息前，应向个人信息主体告知所提供产品或服务的核心业务功能及所必需收集的个人敏感信息，并明确告知拒绝提供或拒绝同意将带来的影响。应允许个人信息主体选择是否提供或同意自动采集。

规范还对“明示同意”做出解释，即个人信息主体通过书面声明或主动做出肯定性动作，对其个人信息进行特定处理做出明确授权的行为。并认为肯定性动作包括个人信息主体主动作出声明（电子或纸质形式）、主动勾选、主动点击“同意”、“注册”、“发送”、“拨打”等。

（3）测评方式

这一部分测评考察移动金融交互类 APP 产品在收集用户财产与身份信息时（即收集上述信息开始前），针对收集规则、用途、使用方式等内容的文本（或包含在用户协议中的隐私政策）征求用户“明示同意”的方式。

根据《个人信息安全规范》附件中的划分，银行卡信息与身份证信息都属于个人敏感信息。根据要求，收集个人敏感信息时，应取得个人信息主体的明示同意。此处的明示同意指，个人信息主体通过书面声明或主动做出肯定性动作，对其个人信息进行特定处理做出明确授权的行为。

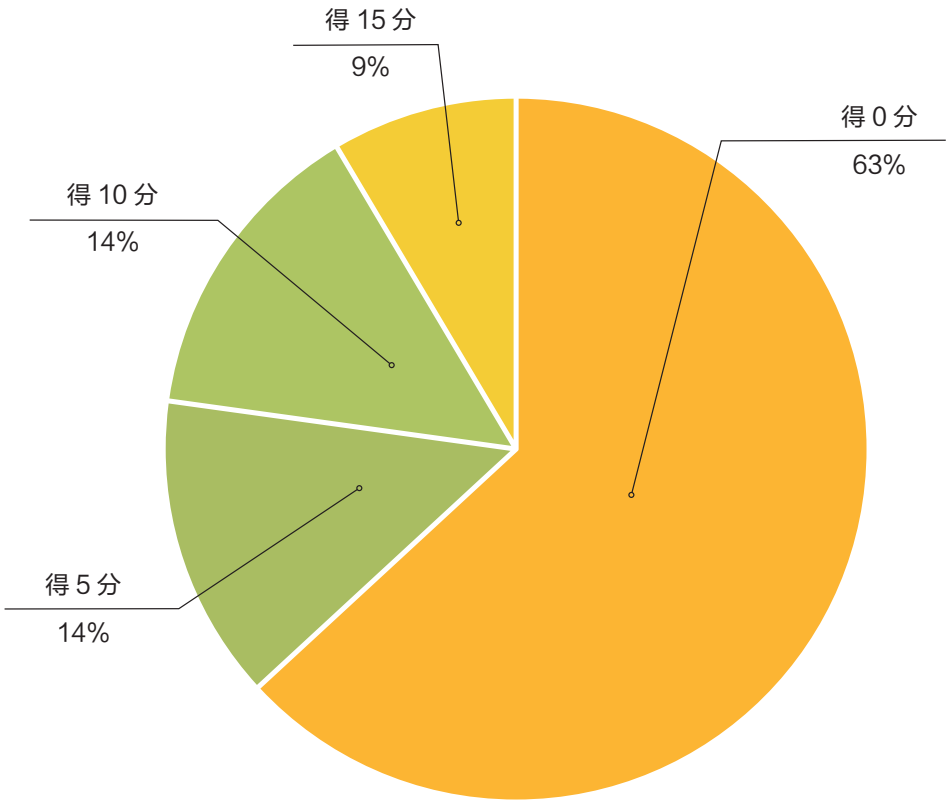
测评根据结果分为四种不同的“明示同意”方式，即：（1）未提供相关文本协议（得 0 分）；（2）有协议但不可勾选（得 5 分）；（3）有协议但已默认勾选同意（得 10 分）；（4）协议提供勾选框并需要用户主动手动同意（得 15 分）。

需要特别提醒的是：1. 本次测评取证的时间为 2018 年 1 月 12 日至 13 日，参与测评的 APP 在这一日期前或日期后所进行的有关修改情况不考虑在本次测评报告内。2. 本报告只讨论身份与财产信息收集时的明示同意，注册、共享或其他场景下的明示同意不在本次测评的范围内。

（4）测评结果

经测试，200 家 APP 的明示同意状况数据统计结果如下：

明示同意方式	APP 个数	举例
（1）未提供相关文本协议（得 0 分）	126	拍拍贷、平安普惠、陆金所等
（2）有协议但不可勾选（得 5 分）	28	支付宝、京东金融、趣店等
（3）有协议但已默认勾选同意（得 10 分）	29	小米金融、拉卡拉、苏宁金融等
（4）协议提供勾选框并需要用户主动手动同意（得 15 分）	17	招联金融、悟空理财、中融投等



【图 4. 财产与身份信息收集合规程度百分比】

根据《个人信息安全规范》，用户对隐私政策的明示同意需有“肯定性动作”，因此下述部分主要按照这一点来划分。

由统计结果来看，200 家 APP 获取同意的方式各异，其中：

1 ■ 有 126 家 APP 未提供相关文本协议，而是直接收集了用户的身份与财产信息。如下图左为宅 e 贷 ,右为陆金所 ,这两款 APP 在收集用户敏感信息时未做到明示同意。

2 ■ 测试中有 28 款 APP 都有相关的协议文本，但用户不可勾选（红色标出部分）。此种情形的举例如下图，左为京东金融，右为爱钱进的个人敏感信息收集页面。这类 APP 在页面中提供了相关文本协议，但直接注明用户已经阅读并同意了相关协议，可以被看做被动同意。需要说明的是，根据《个人信息安全规范》，肯定性动作包括个人信息主体主动作出声明（电子或纸质形式）、主动勾选、主动点击“同意”、“注册”、“发送”、“拨打”等。因此，这类做法可以被认为是合规的，只是将用户开通的行为与信息收集的同意动作合二为一。

3 ■ 有 29 家 APP 试图给用户以选择权，他们虽然在注册页面的隐私政策前加入一个选择框，可供打勾。但遗憾的是，却在框中默认打好了勾，帮助用户做出了选择。此种类型 APP 举例如下，左为拉卡拉相关页面，右为融 360。

4 ■ 在接受测试的 200 家 APP 中，有 17 家 APP 在注册页面中隐私政策前设置了勾选框，并默认不同意。这种方式可以认为给予了用户充分的知情选择权，在这部分测评中得到满分 15 分。如下图，左为招联金融相关页面，右为中融投。

（5）结论

在测评的 200 家 APP 中，在收集用户财产与身份信息时，有 63% 的 APP 没有提供相应的协议文本。14% 的 APP 选择用“点击注册即表示同意”或“我已经阅读并知晓”的被动接受方式作为收集个人敏感信息的告知方式；另有 14.5% 的 APP 提供了相关政策文本，并提供了勾选框，但设定为默认同意；只有 8.5% 的 APP 在获得用户同意时使用了弹出窗口或者默认不同意的方式，合理地给予了用户选择权。

从测评的数据来看，超过半数的移动金融交互类 APP 产品对于用户个人信息与用户个人敏感信息未做区分，在收集个人敏感信息时，对于收集的用途和必要性未做提醒，可以被看做无视用户个人敏感信息的安全。200 款 APP 中，只有 8.5% 的 APP 能够做到完全合规地收集用户个人敏感信息。

作为个人敏感信息，财产信息、实名身份信息一旦泄露，造成的结果不堪设想。移动金融交互类 APP 产品相比其他领域 APP，会更频繁地使用这类信息，如果在收集时都不能做到合法合规，那么，其安全性与对个人敏感信息的重视程度都值得用户警惕。

四、总成绩与排行

本测试的最终结果为上述三个部分测评的分数总和（满分为 140 分），为了便于理解，总分最终再转化为百分制。如一款借贷类 APP 第一部分测评的分数为 70 分；第二部分为 15 分；第三部分为 8 分，最终三项加总为 93 分。93 分转化为百分制成绩：93/140*100=66 分。这一款应用最终个人信息安全的分数就为 66 分。

对比三部分的分数来看，200 款移动金融交互类 APP 产品隐私政策合规程度普遍较高，这是由于网络安全法的实施与四部委对于十款应用隐私政策的测评，推动了 APP 隐私政策合规程度的整体提升。

相较而言，APP 获取敏感隐私权限和收集敏感信息时的合规程度较低。这一方面是由于应用开放商没有对于个人信息与个人敏感信息的区分意识，另一方面是由于与敏感权限相关的法律法规较少。尽管《个人信息安全规范》中针对个人敏感信息的保护作出相关规定，但需要注意的是，《个人信息安全规范》是一部国家标准，不具有强制力。也就是说，这些合规的要求只能通过企业自愿遵守或相关执法部门参照执法以具备约束力。

以下是本次测评的 200 款移动金融交互类 APP 产品的总成绩排名：

排名	APP	隐私政策合规	隐私权限获取合规	财产身份信息收集合规	总分
1	京东金融	95	8.3	5	77.4
2	支付宝	95	4.2	5	74.4
3	小米金融	82	8.3	10	71.7
4	借贷宝	77	8.3	15	71.7
5	桔子理财	68	16.7	5	64.0
6	东方汇财富	55	16.7	15	61.9
7	人人贷	82	4.2	0	61.5
8	挖财	62	8.3	15	61.0
9	拉卡拉	66	8.3	10	60.2
10	平安普惠	80	4.2	0	60.1
11	合拍在线	53	25.0	5	59.3
12	开鑫理财	47	20.8	15	59.2
13	百度钱包	74	8.3	0	58.8
14	麦子金服财富	69	12.5	0	58.2
15	中业兴融	59	16.7	5	57.6
16	聚金资本	68	12.5	0	57.5
17	会分期	75	4.2	0	56.5
18	小九金服	42	20.8	15	55.6
19	知商金融	60	12.5	5	55.4
20	分期乐	64	8.3	5	55.2
21	招商贷	56	20.8	0	54.9
22	百金贷	56	20.8	0	54.9
23	小猪理财	45	20.8	10	54.2
24	地标金融	44	16.7	15	54.0
25	多赢金融	58	16.7	0	53.3
26	合盘贷	58	16.7	0	53.3
27	我来贷	66	8.3	0	53.1
28	信融财富	34	25.0	15	52.9
29	365 易贷	51	12.5	10	52.5
30	聚财猫	64	4.2	5	52.3
31	中融投	45	12.5	15	51.8
32	金投行	37	25.0	10	51.4
33	微贷网	51	20.8	0	51.3
34	卡卡贷（专业版）	55	16.7	0	51.2

排名	APP	隐私政策合规	隐私权限获取合规	财产身份信息收集合规	总分
35	生菜金融	45	16.7	10	51.2
36	微众银行	59	12.5	0	51.1
37	可溯金融	59	12.5	10	51.1
38	希望金融	40	20.8	10	50.6
39	银谷在线	54	16.7	0	50.5
40	民贷天下	44	16.7	10	50.5
41	国泰·惠民益贷	34	20.8	15	49.9
42	君融贷	47	12.5	10	49.6
43	洋钱罐	61	8.3	0	49.5
44	泰然金融	60	4.2	5	49.4
45	步步盈	48	20.8	0	49.2
46	网信理财	64	4.2	0	48.7
47	普汇理财	51	16.7	0	48.3
48	新升贷	46	16.7	5	48.3
49	91 旺财	54	8.3	5	48.1
50	恒大金服	49	12.5	5	47.5
51	2345 贷款王	58	8.3	0	47.4
52	付融宝	58	8.3	0	47.4
53	有融网	35	20.8	10	47.0
54	拓道金服	49	16.7	0	46.9
55	新联在线	53	12.5	0	46.8
56	华赢贷	53	12.5	0	46.8
57	多多理财	48	12.5	5	46.8
58	乐金所	43	12.5	10	46.8
59	招联金融	42	8.3	15	46.7
60	360 你财富	52	8.3	5	46.7
61	达人贷	40	25.0	0	46.4
62	恒信易贷	44	20.8	0	46.3
63	链链金融	48	16.7	0	46.2
64	汇盈金服	43	16.7	5	46.2
65	e 路同心	43	16.7	5	46.2
66	首 E 家	41	12.5	10	45.4
67	抱财网	55	8.3	0	45.2
68	e 融所	35	12.5	15	44.6

排名	APP	隐私政策合规	隐私权限获取合规	财产身份信息收集合规	总分
69	盈盈理财	50	12.5	0	44.6
70	万家贷	39	8.3	15	44.5
71	杉易贷投资	37	25.0	0	44.3
72	银票网	49	12.5	0	43.9
73	小牛在线	43	8.3	10	43.8
74	钱盆网	40	20.8	0	43.5
75	前金融	40	20.8	0	43.5
76	金联储金服	48	12.5	0	43.2
77	小微时贷	37	8.3	15	43.1
78	苏宁金融	46	4.2	10	43.0
79	搜易贷	39	20.8	0	42.7
80	微车融	43	16.7	0	42.6
81	懒财网	38	16.7	5	42.6
82	金信宝	47	12.5	0	42.5
83	恩科 e 贷	47	12.5	0	42.5
84	钱爸爸	51	8.3	0	42.4
85	理财农场	46	8.3	5	42.4
86	博金贷	36	12.5	10	41.8
87	道口贷	41	16.7	0	41.2
88	果树财富	41	16.7	0	41.2
89	米庄理财	35	12.5	10	41.1
90	融贝网	35	12.5	10	41.1
91	宝象金融	49	8.3	0	41.0
92	零用贷	39	8.3	10	41.0
93	中国农业银行	39	8.3	10	41.0
94	分利宝	53	4.2	0	40.8
95	前海惠农	36	20.8	0	40.6
96	轻易贷	44	12.5	0	40.4
97	钱保姆	52	4.2	0	40.1
98	乐享宝	35	20.8	0	39.9
99	友金所	29	16.7	10	39.8
100	人人聚财	38	12.5	5	39.6
101	元宝 365	33	12.5	10	39.6
102	安心贷	47	8.3	0	39.5

排名	APP	隐私政策合规	隐私权限获取合规	财产身份信息收集合规	总分
103	借么 - 信和大金融	47	8.3	0	39.5
104	汇诚金服	47	8.3	0	39.5
105	投哪网理财	41	4.2	10	39.4
106	钱多多	29	20.8	5	39.2
107	九斗鱼	50	4.2	0	38.7
108	白菜金融	37	16.7	0	38.3
109	小赢理财	41	12.5	0	38.2
110	鑫合汇网贷	41	12.5	0	38.2
111	蜡笔分期	41	12.5	0	38.2
112	信广立诚贷	41	12.5	0	38.2
113	金桥梁	40	8.3	5	38.1
114	乐居财富	36	16.7	0	37.6
115	嘉石榴理财	36	16.7	0	37.6
116	小油菜金服	36	16.7	0	37.6
117	信用钱包	40	12.5	0	37.5
118	银豆网	35	12.5	5	37.5
119	积木盒子	30	12.5	10	37.5
120	聚宝匯	44	8.3	0	37.4
121	易通贷	35	16.7	0	36.9
122	钱香金融	24	12.5	15	36.8
123	汇通易贷	34	16.7	0	36.2
124	宜聚网	38	12.5	0	36.1
125	投复利	27	8.3	15	36.0
126	利得高端理财	33	16.7	0	35.5
127	宝点理财	33	16.7	0	35.5
128	银巴克理财	37	12.5	0	35.4
129	飞贷	37	12.5	0	35.4
130	好收益	37	12.5	0	35.4
131	宜借款	41	8.3	0	35.2
132	有利网	23	20.8	5	34.9
133	捷信消费金融	36	12.5	0	34.6
134	马上消费金融	36	12.5	0	34.6
135	小鸡理财	36	12.5	0	34.6
136	陆金所	40	8.3	0	34.5

排名	APP	隐私政策合规	隐私权限获取合规	财产身份信息收集合规	总分
137	投融家	44	4.2	0	34.4
138	理想宝	48	0.0	0	34.3
139	和信贷	20	12.5	15	33.9
140	爱钱进	30	12.5	5	33.9
141	闪银	39	8.3	0	33.8
142	网利宝	33	4.2	10	33.7
143	融 360	32	4.2	10	33.0
144	众易贷	28	16.7	0	31.9
145	快快贷	28	16.7	0	31.9
146	和包	32	12.5	0	31.8
147	钱牛牛	32	12.5	0	31.8
148	冠 e 通	32	12.5	0	31.8
149	拍拍贷	36	8.3	0	31.7
150	PP money	36	8.3	0	31.7
151	闪电借款	36	8.3	0	31.7
152	普惠家	36	8.3	0	31.7
153	信而富	31	12.5	0	31.1
154	省呗	31	12.5	0	31.1
155	中融宝	31	12.5	0	31.1
156	向上金服	35	8.3	0	31.0
157	悟空理财	24	4.2	15	30.8
158	温商贷	34	8.3	0	30.2
159	铜板街	24	8.3	10	30.2
160	淘淘金	28	12.5	0	28.9
161	信用宝	31	8.3	0	28.1
162	欢乐合家	35	4.2	0	28.0
163	互惠理财	21	16.7	0	26.9
164	凤凰金融	29	8.3	0	26.7
165	念钱安	28	8.3	0	26.0
166	51 信用卡	32	4.2	0	25.8
167	爱投金融	18	12.5	5	25.4
168	你我贷借款	27	8.3	0	25.2
169	中国工商银行	27	8.3	0	25.2
170	亿宝贷	31	4.2	0	25.1

排名	APP	隐私政策合规	隐私权限获取合规	财产身份信息收集合规	总分
171	易港金融	0	25.0	10	25.0
172	团贷网	26	8.3	0	24.5
173	郑投网理财	26	8.3	0	24.5
174	点融网	24	8.3	0	23.1
175	人众金服	24	8.3	0	23.1
176	合众 e 贷	19	8.3	5	23.1
177	口袋理财	22	8.3	0	21.7
178	红岭创投	16	12.5	0	20.4
179	金融圈	16	12.5	0	20.4
180	金银猫	20	8.3	0	20.2
181	中国银行	0	12.5	15	19.6
182	聚车金融	0	16.7	10	19.0
183	宜贷网	0	12.5	10	16.1
184	珠宝贷	0	16.7	5	15.5
185	聚爱财	17	4.2	0	15.1
186	来存吧票据理财	0	20.8	0	14.9
187	诚汇通	0	20.8	0	14.9
188	绿化贷	0	20.8	0	14.9
189	隆金宝	0	16.7	0	11.9
190	中兴财富	0	16.7	0	11.9
191	精融汇	0	16.7	0	11.9
192	58 车贷	0	16.7	0	11.9
193	趣店	0	8.3	5	9.5
194	钱内助	0	12.5	0	8.9
195	渝金所	0	12.5	0	8.9
196	短融网	0	8.3	0	6.0
197	E 都市钱包	0	8.3	0	6.0
198	中潮金服	0	8.3	0	6.0
199	中国建设银行	0	8.3	0	6.0
200	三信理财	0	4.2	0	3.0

五、声明与保留

（1）本次测评主要考察移动金融交互类 APP 产品的个人信息收集合规程度，不包括个人信息的保存、保护、分享等环节。

（2）采样时间截止 2018 年 2 月 20 日。我们注意到各个企业的隐私政策可能不时调整，因此本此抽样调查仅对截止日的隐私政策样本负责。

（3）在打分环节，我们通过交叉测评、技术介入等方式打分，后进行汇总。尽管我们力求能够尽量客观地反映某一公司在某一项的情况，但并不排除在打分时，包含评分人员的主观看法和印象。

（4）一方面，我们将继续完善测评标准，定期查看企业隐私政策的更新情况，扩大领域和评估范围，对更多互联网企业的隐私政策进行测评。我们希望推动更多社会力量，和我们一起敦促企业完善隐私保护措施，满足用户的知情需求，做好个人信息保护工作。同时我们也希望金融类产品在合法合规的前提下蓬勃发展，成为大数据产业发展中安全的中坚力量。

联合发布方：

南都个人信息保护研究中心

中国人民大学金融科技与互联网安全研究中心

法律顾问：北京玺泽律师事务所

我们也欢迎您向我们提供您的观点，2018 年，在个人信息保护领域，什么问题最值得关注。可以通过以下方式与我们联系：ppa-nandu01@163.com 或者关注我们的微信公众号“隐私护卫队”直接留言。