



公司及并购法律评述  
2019年3月

**上海**  
上海市银城中路68号  
时代金融中心16楼和19楼  
邮编: 200120  
电话: +86 21 3135 8666  
传真: +86 21 3135 8600

**SHANGHAI**  
16F/19F, ONE LUJIAZUI  
68 Yin Cheng Road Middle  
Shanghai 200120 P.R.China  
T: +86 21 3135 8666  
F: +86 21 3135 8600

**北京**  
北京市建国门北大街8号  
华润大厦4楼  
邮编: 100005  
电话: +86 10 8519 2266  
传真: +86 10 8519 2929

**BEIJING**  
4F, China Resources Building  
8 Jianguomenbei Avenue  
Beijing 100005 P.R.China  
T: +86 10 8519 2266  
F: +86 10 8519 2929

**香港**  
香港中环皇后大道中5号  
衡怡大厦27楼  
电话: +852 2592 1978  
传真: +852 2868 0883

**HONG KONG**  
27F, Henley Building  
5 Queen's Road Central  
Central, Hong Kong  
T: +852 2592 1978  
F: +852 2868 0883

**伦敦**  
1F, 3 More London Riverside  
London SE1 2RE  
United Kingdom  
T: +44 (0)20 3283 4337  
D: +44 (0)20 3283 4323

**LONDON**  
1F, 3 More London Riverside  
London SE1 2RE  
United Kingdom  
T: +44 (0)20 3283 4337  
D: +44 (0)20 3283 4323

[www.llinkslaw.com](http://www.llinkslaw.com)

[master@llinkslaw.com](mailto:master@llinkslaw.com)

## 监管思路也需因势而变——简评 App 安全认证制度及应对建议

作者: 潘永建 | 邓梓珊

央视3·15晚会重点曝光了App泄露个人隐私信息的案例,将民众目光聚焦于移动互联网的个人信息安全问题。同日,市场监管总局、中央网信办发布了《关于开展App安全认证工作的公告》(“《App认证公告》”),并附上国家认证认可监督管理委员会发布的《移动互联网应用程序(App)安全认证实施规则》(“《App认证规则》”)以规范App收集、使用用户信息特别是个人信息的行为,加强个人信息安全保护。本文将在对《App认证公告》和《App认证规则》进行分析解读的基础上,为企业如何通过App合规收集、使用用户个人信息提出建议。

### 一. 政策背景

2019年开年以来,国家有关部门针对App收集、使用用户个人信息陆续出台了一系列治理政策、指南、实施规则(见下表)。App用户个人信息安全已成为监管焦点。

如您需要了解我们的出版物,  
请与下列人员联系:

**郭建良**: +86 21 3135 8756  
[Publication@llinkslaw.com](mailto:Publication@llinkslaw.com)

**通力律师事务所**  
[www.llinkslaw.com](http://www.llinkslaw.com)

**免责声明**: 本出版物仅代表作者本人观点,不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

## 监管思路也需因势而变——简评 App 安全认证制度及应对建议

2019年1月23日	中央网信办、工信部、公安部、市场监管总局	《关于开展 App 违法违规收集使用个人信息专项治理的公告》
2019年3月1日	全国信息安全标准化技术委员会、中国消费者协会、中国互联网协会、中国网络空间安全协会(以下简称“App 专项治理工作组”)	《App 违法违规收集使用个人信息自评估指南》
2019年3月13日	市场监管总局、中央网信办	《关于开展 App 安全认证工作的公告》
2019年3月13日	国家认证认可监督管理委员会	《移动互联网应用程序(App)安全认证实施规则》

值得注意的是, App 专项治理工作要求 App 运营者进行自查;同时,从公众监督的角度出发, App 专项治理工作组设立了“App 个人信息举报”微信公众号,鼓励 App 用户对 App 违法违规收集使用个人信息的行为进行举报;此次《App 认证公告》以及《App 认证规则》也并未要求所有的 App 都必须进行安全认证。从这种态势变化可以看出,监管部门在加强事后处罚的同时,治理方式逐渐趋于多样化,对于个人信息违法违规的问题越来越注重事前监管;且辅以引导的方式,鼓励 App 运营者进行合规自查主动提升个人信息保护水平。此次发布的《App 认证公告》旨在鼓励 App 运营者主动进行 App 安全检测、通过 App 安全认证,并鼓励搜索引擎、应用商店等明确标识并优先推荐已通过认证的 App,为 App 用户提供安全放心的移动互联网环境。《App 认证规则》则对检测认证的具体程序作出了详细的指引。

## 二. 重点提示

### 1. 认证适用范围: 移动互联网应用程序

根据网信办于 2016 年 6 月 28 日发布的《移动互联网应用程序信息服务管理规定》,移动互联网应用程序指通过预装、下载等方式获取并运行在移动智能终端上、向用户提供信息服务的应用软件。而根据工信部于 2016 年 12 月 16 日发布的《移动智能终端应用软件预置和分发管理暂行规定》,移动智能终端指接入公众移动通信网络、具有操作系统、可由用户自行安装和卸载应用程序的移动终端产品。由此可见,除智能手机以外,其他移动通信终端的应用程序也可以进行 App 安全认证。

### 2. 认证依据: GB/T 35273《信息安全技术个人信息安全规范》

《App 认证公告》以及《App 认证规则》第 2 条明确规定安全认证依据为《中华人民共和国网

## 监管思路也需因势而变——简评 App 安全认证制度及应对建议

络安全法》《中华人民共和国认证认可条例》、GB/T 35273《信息安全技术 个人信息安全规范》(“《个人信息安全规范》”)及相关标准、规范。由于《网络安全法》的配套法规一直未出台,中国亦未公布个人信息保护的综合性法律法规,《个人信息安全规范》自公布以来成为网络运营者进行个人信息的收集、使用、处理及其他合规管理工作的重要指引。《个人信息安全规范》作为推荐性国标,已多次在监管部门的公开文件中被提到,足见其重要性。因此,尽管《个人信息安全规范》为推荐性国标,企业不应掉以轻心,对其在个人信息合规中的落实执行而持犹疑观望的态度。

### 3. 认证模式及流程: 技术验证、现场核查、获证后监督

App 安全认证的主要程序为: 认证申请→认证受理→技术验证→现场审核→认证决定。从 App 认证申请方需提交的文件来看,申请前申请方还需要对是否符合认证的要求,即对照《个人信息安全规范》,进行自我评价并提交自我评价结果。同一名称的 App 还需区分不同版本号、操作系统平台进行分单元申请认证。即使顺利通过了安全认证,还需在认证证书有效期内持续对 App 是否符合认证进行自我评价;在特定情形发生时向认证机构提交自我评价报告;认证机构同时也会对获证 App 和 App 运营者持续实施日常监督以及专项监督。除此之外,《App 认证规则》还就认证时限,结果申诉,限期整改,认证的暂停、撤销和注销、证书及标志的使用和管理作出了规定,整体流程较为完善。

### 4. 认证后优势: 可获优先推荐

根据《App 认证规则》,通过 App 安全认证的 App 运营者将获发认证证书,获得在获证 App 上使用规定认证标志的授权。《App 认证公告》鼓励搜索引擎、应用商店等明确标识并优先推荐已通过认证的 App。

App 安全认证的程序具有一定的复杂性,且包含了获证后管理的完整流程。能够获得认证的 App 运营者应当具有相当的合规意识及管理能力,其在承担更多责任的同时也必能赢得广大用户的认可。

## 三. 合规建议

《App 认证规则》明确指出,通过认证并不能免除获证 App 运营者对获证 App 承担的法律 responsibility。此处所指的法律 responsibility 在《刑法》《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》《网络安全法》《消费者权益保护法》《移动互联网应用程序信息服务管理规定》、《个人信息安全规范》等法律法规、国家标准中均有体现。违法收集、使用或提供个人信息不仅可能导致民事责任或

## 监管思路也需因势而变——简评 App 安全认证制度及应对建议

行政责任，还有可能导致刑事责任，并可能面临最高七年有期徒刑的刑罚。为帮助 App 运营者更好地理解个人信息收集使用的合规要求，我们结合了一些近期的热门案例以及监管态势，提出如下合规建议<sup>1</sup>：

1. 进行内部自查，明确 App 运营过程中需要收集的、实际收集的个人信息范围，并对照行政法律、刑事法律规定进行个人信息的判定、甄别和归类；
2. 完善隐私政策的形式、内容；适当采取增强式告知；提供各项与个人信息有关的功能应以用户为中心；
3. App 运营者收集、使用个人信息应当遵循合法、正当、必要的原则，获取用户知情同意；避免使用“一揽子”同意的方式；避免使用默示同意；
4. 对未成年人提供特殊保护。建立年龄认证和识别系统，对于需要未成年人或其监护人明示同意的情况进行显著提示；设置筛查甄别机制进行事后复查；
5. 避免过度收集信息。收集的个人信息类型应与实现产品或服务的业务功能有直接关联；做到“最低频率”与“最少数量”的要求；对个人敏感信息采取更高层次的合规措施；根据个人信息与实现各项功能之间的因果关系区分产品或服务的核心功能与附加功能，并确保用户拒绝提供个人信息时能够继续使用与该部分个人信息无关的业务功能；
6. 告知如何使用自动数据收集工具；适度收集用户的网络活动信息；向用户提供限制自动工具进行数据收集方法和详细的指导；
7. 注意域外法律，如欧盟《通用数据保护条例》的适用。

## 四. 结语

《App 认证公告》以及《App 认证规则》对实施 App 安全认证的主体、申请认证的模式和程序，App 运营者的主要义务和责任作出了规定，但对于一些具体操作事宜仍需相关部门填补空白。例如申请材料中需包含的“自我评价结果”应采取何种形式、包含何种内容；获证后的自我评价应当如何进行，以何种频率进行；认证机构是否有权对于不同的 App 授予不同有效期的认证证书，证书到期是否可以申请续期换证；《App 认证规则》第 4.3.2 和 4.4.1 所指的“技术验证规范”和“现场审核规范”何时制定公布等。

## 监管思路也需因势而变——简评 App 安全认证制度及应对建议

3·15 晚会曝光了“Wifi 探针”技术，让我们意识到目前新兴技术在悄无声息地肆意攫取个人信息，让人防不胜防。然而现实情况是，类似“Wifi 探针”这样的技术只会越来越多，越来越使人无法察觉防范。正所谓“技术无罪，商业有德”。随着物联网、区块链、大数据开发挖掘等各项技术的井喷式涌现和发展，对于用户个人信息及隐私数据的保护越发有赖于商家自身的道德意识、合规管理能力。正因如此，执法部门也在不断加强执法力度的同时，填补法律上的空白，创新治理思路和方法。App 运营者，尤其是那些依赖用户个人信息的 App 的运营者，应该将个人信息的合规作为所有合规制度的重中之重。合法合规地收集使用个人信息，才能提高用户粘度和好感度，促进 App 运营者长期可持续发展。

## 监管思路也需因势而变——简评 App 安全认证制度及应对建议

如需进一步信息，请联系：

<b>作者</b>	
<b>潘永建</b> 电话: +86 21 3135 8701 david.pan@linkslaw.com	
<b>上海</b>	
<b>俞卫锋</b> 电话: +86 21 3135 8686 david.yu@linkslaw.com	<b>刘贇春</b> 电话: +86 21 3135 8678 bernie.liu@linkslaw.com
<b>佘铭</b> 电话: +86 21 3135 8770 selenashe@linkslaw.com	<b>娄斐弘</b> 电话: +86 21 3135 8783 nicholas.lou@linkslaw.com
<b>钱大立</b> 电话: +86 21 3135 8676 dali.qian@linkslaw.com	<b>孔焕志</b> 电话: +86 21 3135 8777 kenneth.kong@linkslaw.com
<b>吴炜</b> 电话: +86 21 6043 3711 david.wu@linkslaw.com	<b>潘永建</b> 电话: +86 21 3135 8701 david.pan@linkslaw.com
<b>姜琳</b> 电话: +86 21 6043 3710 elyn.jiang@linkslaw.com	
<b>北京</b>	
<b>俞卫锋</b> 电话: +86 10 8519 2266 david.yu@linkslaw.com	<b>刘贇春</b> 电话: +86 10 8519 2266 bernie.liu@linkslaw.com
<b>杨玉华</b> 电话: +86 10 8519 1606 yuhua.yang@linkslaw.com	
<b>香港(与方緯谷律师事务所联营)</b>	
<b>俞卫锋</b> 电话: +86 21 3135 8686 david.yu@linkslaw.com	<b>吕红</b> 电话: +86 21 3135 8776 sandra.lu@linkslaw.com
<b>伦敦</b>	
<b>杨玉华</b> 电话: +44 (0)20 3283 4337 yuhua.yang@linkslaw.com	

© 本篇文章独家授权 LexisNexis 律商联讯发布，未经许可，不得转载。

<sup>1</sup> 热门案例、以及合规建议展开内容请见通力律师事务所的法评文章《App: 从“予取予求”到“取之有道”——简析 App 运营者收集使用个人信息的合规要点》。

**免责声明：**本出版物仅代表作者本人观点，不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。