



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

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

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

伦敦
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

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

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

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

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

master@llinkslaw.com

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

作者: 潘永建 | 朱晓阳 | 邓梓珊

2019 年 2 月 27 日, 美国联邦贸易委员会(Federal Trade Commission, “FTC”)发布公告称, 在线视频 APP, Musical.ly(现已合并入抖音海外版 Tik Tok¹)的运营方同意就 FTC 有关其违反美国儿童在线隐私保护法(Children’s Online Privacy Protection Act, “COPPA”)的指控与 FTC 达成和解并支付 570 万美元。根据 FTC 对 Musical.ly 的指控, Musical.ly 明知其用户中存在大量 13 岁以下儿童, 在收集相关儿童的个人信息时未告知儿童父母, 未征得儿童父母的同意, 亦未根据相关儿童父母的要求删除儿童的个人信息。Musical.ly 上述行为违反了 COPPA。

因 570 万美元是 FTC 对侵犯儿童隐私行为开出的最大“罚单”, 该案迅速得到高度关注。事实上, 因违反个人信息保护法律而被处罚, 抖音并不“孤单”。2019 年才刚刚进入第三个月, 因个人信息违规而“惹祸上身”的境内外公司已经不在少数。

2019 年 1 月 21 日, 法国数据保护监管机构 La Commission nationale de l’informatique et des libertés (“CNIL”)因 Google

For more Llinks publications, please contact:

Roy Guo: +86 21 3135 8756
Publication@llinkslaw.com

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

通力律师事务所
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。

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

违反欧盟通用数据保护条例(General Data Protection Regulation, “GDPR”), 对其处以 5000 万欧元的罚款。根据 CNIL 的公告, 对 Google 的处罚原因主要是两点: 第一, Google 没有对其如何处理用户个人信息进行明确、完整的说明; 第二, Google 获取用户有关将其个人信息用于个性化广告定制的同意不明确、具体。

根据欧盟其他数据保护机构的公告, Facebook 目前正在接受爱尔兰数据保护委员会(Irish Data Protection Commission)对其进行的 10 项有关其违反 GDPR 的调查, 其中既包括对 Facebook 本身的调查也包括对其旗下品牌 Whatsapp 及 Instagram 的调查。此外, 欧盟数据保护机构对 Apple, 微软及 Twitter 目前也都在进行调查。对于这些巨头违反个人信息保护法律的处罚可能在今年晚些时候做出。

2019 年 2 月 16 日, 有微博用户爆出其在京东金融 APP 安卓版的缓存文件中发现了其通过手机截屏工具以及其他拍照 APP 生成的图片, 怀疑京东金融 APP 存在私自收集、上传用户照片, 侵犯用户隐私的行为。京东金融对此进行内部自查后得出的结论是“京东金融 APP 在功能开发上存在技术问题”, 并且发表了官方致歉声明, 表示“从未想过未经用户授权获取用户图片……之前没有, 未来也不会私自上传用户图片”。虽然目前尚不清楚监管机关是否会对本次京东金融的“技术问题”进行调查或处罚, 但这一事件进一步引发了公众对 APP 收集使用个人信息的合规问题的关注。

上述案例表明, 随着监管的加强、执法技术的提高以及用户个人信息保护意识增长, APP 运营者违法违规收集、使用个人信息牟利且不承担责任的时代已经一去不复返。

一、法律和监管

近年来, 随着大数据相关技术的发展及对数据价值的不断攫取, 各行各业的经营者对于用户个人信息的“饥渴”和依赖导致了违法违规收集、使用个人信息行为的泛滥。为了应对及遏制这种现象, 我国针对个人信息保护的立法及相关执法也在这一阶段呈现了“井喷”的态势。

1. 刑事法律

大多数经营者可能对违法收集、使用或提供个人信息的行政责任“烂熟于心”, 认为违反了相关法律不过是警告、整顿或罚款了事。殊不知, 自 2015 年起个人信息保护已经被纳入了刑法, 违反刑法相关规定者将承担刑事责任, 并可能面临最高七年有期徒刑的刑罚。

《刑法》第 253 条之一规定, “违反国家有关规定, 向他人出售或者提供公民个人信息, 情节严重的, 处三年以下有期徒刑或者拘役, 并处或单处罚金; 情节特别严重的, 处三年以上七年以下有期徒刑, 并处罚金”, 同时规定, “窃取或者以其他方式非法获取公民个人信息的”, 依照前

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

款的规定处罚。

最高人民法院及最高人民检察院于 2017 年 5 月 8 日发布《关于办理侵犯公民个人信息罪刑事案件适用法律若干问题的解释》，对于侵犯公民个人信息罪的认定及刑罚做出了进一步的明确解释。其中规定，《刑法》第 253 条之一中的“情节严重”包括“非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的”、“非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的”，及非法获取、出售或者提供前两项规定以外的公民个人信息五千条以上的，或违法所得五千元以上的；而“情节特别严重”的情形包括侵犯公民个人信息的数量，或者违法所得的数额达到“情节严重”中规定的标准的十倍以上的。按照该解释，在提供服务过程中获得的公民个人信息出售或者提供给他人，上述刑事责任的数量或者数额标准减半。

2. 民事法律

《民法总则》第 111 条规定，“自然人的个人信息受法律保护。任何组织和个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输个人信息，不得非法买卖、提供或者公开他人个人信息”。

目前我国法律虽然尚未将“个人信息权”规定为一项法定权利，但根据《民法总则》的规定，个人信息主体无疑享有其个人信息免受违法违规收集、使用的权益。对于违反法律规定，侵犯自然人个人信息权益的，个人信息主体可要求其承担相应民事责任，包括但不限于停止侵害、排除妨害、赔偿损失、消除影响、恢复名誉、赔礼道歉等。

此外，个人信息主体对其个人信息的民事权益还可能和其他法定权利发生竞合，例如肖像权、隐私权等，在这种情况下，个人信息主体还可以选择要求侵权人根据侵权责任法的规定，承担侵犯其肖像权、隐私权的侵权责任。

3. 行政法律

目前，行政法律领域可以说是保护个人信息的“主战场”。无论是从法律法规及处罚案件的数量、还是经营者的重视程度，行政法律领域都要远远高于刑事及民事法律领域。

《网络安全法》（“网安法”）对个人信息保护做出了原则性的规定。根据网安法，“网络运营者

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

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”。此外，“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”，且“未经被收集者同意，不得向他人提供个人信息。但是经处理无法识别特定个人且不能复原的除外”。

提到行政领域个人信息保护，就不得不提推荐性国家标准《信息安全技术 个人信息安全规范》(GB/T 35273-2017)(“个人信息国标”)。个人信息国标对“个人信息”做出了明确的定义，同时还提出了“个人敏感信息”的概念，并且针对个人信息的收集、保存、使用及委托处理、共享、转让、公开披露等行为，提出了具体的细化要求。虽然个人信息国标只是推荐性国家标准，其本身并不具有强制力，但需要指出的是，在网安法及其他个人信息保护相关法律缺乏明确的实施细则和标准的情况下，个人信息国标将会被行政及司法机关作为判断事实和构成要件是否满足的依据，从而根据相关法律的规定做出认定和处罚，而经营者将承担相应的民事、行政甚至刑事责任。此外，个人信息国标作为一部推荐性国家标准，其制定的标准一般而言高于法律要求的标准。APP 运营者如果按照个人信息国标的要求履行其个人信息保护的相关义务，可以保证不违反适用的法律、法规，且可以在执法机关进行调查或第三方提出主张时为其提供抗辩。

除网安法及个人信息国标外，众多涉及不同领域或行业的单行法规也对个人信息保护做出了专门规定，例如《全国人民代表大会关于加强网络信息保护的決定》《电信和互联网用户个人信息保护规定》《寄递服务用户个人信息安全管理规定》《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》及《互联网个人信息安全保护指引》等专门针对个人信息保护的法规及规范性文件。除此以外，其他法律法规及规范性文件中也会对其所涉及的个人信息保护作出规定，例如《消费者权益保护法》、《未成年人保护法》、《商业银行法》、《居民身份证法》、《护照法》、《旅游法》、《电子签名法》、《征信管理条例》等均对其管辖范围内的个人信息保护做出了明确的规定。

一个值得注意的趋势是，在加强事后处罚的同时，监管机关对于个人信息违法违规问题也越来越注重事前监管。2019 年 1 月 25 日，中央网信办、工业和信息化部、公安部及市场监督管理总局联合发布了《关于开展 APP 违法违规收集使用个人信息专项治理的公告》(“专项公告”)。专项公告强调了网安法等法律法规提出的收集、使用个人信息的原则性要求，以及各政府主管部门在查处个人信息违法违规行为的职责，并创新性地提出了由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(以上简称“APP 专项治理工作组”)制定 APP 信息规范及违法违规收集个人信息治理评估要点，并组织相关专业机构对用户数量大、与民众生活密切相关的 APP 的隐私政策及个人信息收集使用情况进行评估。同时也鼓励经

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

运营者对其 APP 参照自评估指南(见下文定义)进行自查自纠, 主动提升个人信息保护水平。

APP 专项治理工作组制定了《APP 违法违规收集使用个人信息自评估指南》(“APP 自评估指南”), 从隐私政策文本、APP 收集使用个人信息行为、APP 运营者对用户权利的保障等三大方面对 APP 运营者做出了指引。就隐私政策而言, APP 自评估指南提出了 1)隐私政策的独立性、易读性; 2)清晰说明各项业务功能及所收集个人信息类型; 及 3)清晰说明个人信息处理规则及用户权益保障。针对 APP 收集使用个人信息行为, APP 自评估指南提出了以下要点: 1)收集个人信息应明示收集目的、方式、范围; 2)收集使用个人信息应经用户自主选择同意, 不应存在强制捆绑授权行为; 3)收集个人信息应满足必要性要求。针对 APP 运营者对用户权利的保障, APP 自评估指南提出了两点要求: 1)支持用户注销账号、更正或删除个人信息; 及 2)及时反馈用户申诉。

APP 专项治理工作组还设立了“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。

二、合规建议

本文开篇介绍的相关公司违法违规收集使用个人信息的案例在给 APP 运营者带来警示的同时, 也对如何合法合规地使用个人信息、调整经营方针指明了方向, 明确了个人信息收集使用的边界。

如上所述, 专项公告为 APP 运营者合法合规收集使用个人信息提出了非常明确且具有操作性的指引。根据专项公告, APP 运营者收集使用个人信息时, 不得收集与所提供无关的个人信息; “收集个人信息时要以通俗易懂、简单明了的方式展示个人信息收集使用规则, 并经个人信息主体自主选择同意; 不以默认、捆绑、停止安装使用等手段变相强迫用户授权, 不得违反法律法规和与用户的约定收集使用个人信息。”前述要求其实在网安法, 《消费者权益保护法》, 个人信息国标等法律法规、国家标准中均已有体现。本文以下便结合上述案例及相关法律及监管态势, 提出 APP 运营者个人信息收集使用的若干合规建议。

1. 完善隐私政策

- 1) 隐私政策应尽量简洁、用户友好, 并可使用图表帮助说明。2017 年中央网信办、工信部、公安部、国家标准委四部门联合开展“个人信息保护提升行动”, 其中, “隐私政策专项工作”评审结果中提出, 鼓励企业制定简洁、易懂的隐私政策, 帮助用户迅速找到关键信息。

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

- 2) 用户安装、注册、第一次使用 APP 前应采取增强式告知, 提示关于个人信息收集的核心内容。增强式告知不是隐私政策的全部内容, 但浓缩了隐私政策的核心, 突出用户最关心的信息, 例如收集的个人信息范围、使用目的和使用主体等。
- 3) 以用户为中心, 提供“一站式”撤回和关闭授权, 在线访问、更正、删除用户个人信息, 在线注销账户等功能。主动区分核心功能和附加功能提供用户选择。

2. 获取用户知情同意

- 1) APP 经营者收集、使用个人信息, 应当遵循合法、正当、必要的原则, 明示收集、使用信息的目的、方式和范围, 并经被收集者同意。不得违反法律、法规的规定和双方的约定收集、使用信息。
- 2) 不应通过捆绑 APP 多项业务功能的方式, 要求用户一次性接受并授权同意多项业务功能收集个人信息的请求。
- 3) 避免默示同意。应根据用户主动填写、点击、勾选等自主行为, 作为产品或服务的业务功能开启或开始收集个人信息的条件。

3. 对未成年人提供特殊保护

- 1) 建立年龄认证和识别系统, 或利用真实身份注册验证机制, 有效识别未成年人用户。收集未成年人的个人信息前, 严格要求用户或其监护人明示同意, 进行显著提示; 不满 14 周岁的未成年人, 应征得其监护人的明示同意。
- 2) 设置筛查甄别机制, 及时发现未经同意而收集的未成年人个人信息, 及时删除相关数据。

4. 避免过度收集信息

实践中, 有 APP 运营者将个人信息主体的同意作为使用其个人信息合规性的充分条件。然而, 这一理解是不正确的, 这些 APP 运营者忽视了网安法提出的使用个人信息的“必要”原则, 也忽视了个人信息国标第 5.2 条提出的“最小化要求”。“必要”原则与“最小化要求”意味着:

- 1) 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。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;

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

- 2) 自动采集个人信息的频率应是实现产品或服务的业务功能所必需的最低频率;
- 3) 间接获取个人信息的数量应是实现产品或服务的业务功能所必需的最少数量。

此外, APP 经营者应注意, 个人财产信息、个人健康生理信息与人脸识别信息²等均属于个人敏感信息。收集用户个人敏感信息前, 还应:

- 1) 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;
- 2) 产品或服务如提供其他附加功能, 需要收集个人敏感信息时, 收集前应向个人信息主体逐一说明个人敏感信息为完成何种附加功能所必需, 并允许个人信息主体逐项选择是否提供或同意自动采集个人敏感信息。当个人信息主体拒绝时, 可不提供相应的附加功能, 但不应以此为理由停止提供核心业务功能, 并应保障相应的服务质量。

过度收集个人信息可能导致行政处罚³, 甚至可能构成刑事犯罪⁴。为避免过度收集个人信息, APP 运营者应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。

5. 告知如何使用自动数据收集工具

除用户的基本个人信息外, 用户的网络活动信息, 如用户浏览过的网页、关注过的产品、发布的评论信息等内容都有可能被 APP 内嵌的自动数据收集工具收集而来。

如果在 APP 使用过程中, 或是在 APP 后台运行中有利用自动数据收集工具采集用户网络活动信息的情况, APP 经营者首先应做到适度收集该类网络活动信息, 不应超出与用户所约定的范围和目的收集信息; 另外, APP 经营者应在隐私政策中对使用的技术机制做详细描述, 说明使用自动工具收集个人信息的目的, 并向用户提供限制自动工具进行数据收集的方法和详细的指导。

6. 注意域外法律的适用

除 APP 运营者所在国法律之外, APP 跨国运营与使用可导致 APP 运营者需要遵从外国法律。例

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

如,若 APP 使用者包括欧盟境内公民,则 APP 运营者亦需要遵守 GDPR 的相关规定。GDPR 等域外法律在个人信息定义与保护制度上与中国法律与政策有所不同,在某些领域对运营者提出了更加严格的责任。例如,在作出自动化个人决策和画像(automated individual decision-making and profiling)时,运营者应告知被处理的个人信息的主体相关处理(processing),给予个人信息主体便捷的人工干预或质疑的方法,并定期检查确保自动化个人决策和画像系统按照预定方式运行。

三、结语

合规是所有企业的生命线,同时合规也绝不是对法律法规要求的应付,而是一套能够为企业产生价值的制度。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,为 APP 运营者带来利益。若 APP 运营者继续违法违规使用个人信息,是对用户和法律的蔑视,其结果只能是遭至用户的抛弃和法律的制裁。

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

如需进一步信息, 请联系:

作 者	
潘永建 电话: +86 21 3135 8701 david.pan@linkslaw.com	
上 海	
俞卫锋 电话: +86 21 3135 8686 david.yu@linkslaw.com	刘贇春 电话: +86 21 3135 8678 bernie.liu@linkslaw.com
余 铭 电话: +86 21 3135 8770 selenashe@linkslaw.com	娄斐弘 电话: +86 21 3135 8783 nicholas.lou@linkslaw.com
钱大立 电话: +86 21 3135 8676 dali.qian@linkslaw.com	孔焕志 电话: +86 21 3135 8777 kenneth.kong@linkslaw.com
吴 炜 电话: +86 21 6043 3711 david.wu@linkslaw.com	潘永建 电话: +86 21 3135 8701 david.pan@linkslaw.com
姜 琳 电话: +86 21 6043 3710 elyn.jiang@linkslaw.com	
北 京	
俞卫锋 电话: +86 10 8519 2266 david.yu@linkslaw.com	刘贇春 电话: +86 10 8519 2266 bernie.liu@linkslaw.com
杨玉华 电话: +86 10 8519 1606 yuhua.yang@linkslaw.com	
香 港(与方緯谷律师事务所联营)	
俞卫锋 电话: +86 21 3135 8686 david.yu@linkslaw.com	吕 红 电话: +86 21 3135 8776 sandra.lu@linkslaw.com
伦 敦	
杨玉华 电话: +44 (0)20 3283 4337 yuhua.yang@linkslaw.com	

© 本篇文章独家授权威科先行法律信息库发布, 未经许可, 不得转载。

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。

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

¹ Musical.ly APP 的运营方 MUSICAL.LY INC. 于 2017 年 12 月被抖音的海外主体 ByteDance Ltd. 收购, 同时 Musical.ly APP 的内容也被整合并入抖音海外版 Tik Tok。

² 可参考《信息安全技术 个人信息安全规范》附录 B 个人敏感信息判定。

³ 2018 年 3 月, 支付宝(中国)网络技术有限公司因在“年度账单”中过度要求收集、使用用户个人信息, 被中国人民银行杭州支行以“个人金融信息收集不符合最少、必要原则”及“个人金融信息使用不当”为由处以罚款。

⁴ 《最高人民法院、最高人民检察院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》规定, “违反国家有关规定, 通过购买、收受、交换等方式获取公民个人信息, 或者在履行职责、提供服务过程中收集公民个人信息的, 属于刑法第二百五十三条之一第三款规定的‘以其他方法非法获取公民个人信息’。”