



法律意见书

www.vtlaw.cn

V&T LAW FIRM **万商天勤律师事务所**

北京 BEIJING

北京市朝阳区东四环中路39号
华业国际中心A座3层 100025
F3, Tower A, HUAYE International Center,
No. 39, Dongsihuan Zhonglu,
Chaoyang District, Beijing, 100025
Tel: 86-10-82255588 85711188
Fax: 86-10-82255600

北京 深圳 上海 成都
BEIJING SHENZHEN SHANGHAI CHENGDU

目 录

声 明.....	6
正 文.....	8
一、关注问题	8
问题 3:	8
请发行人说明并在《招股说明书》中补充披露：（1）与 APP 开发者《个推使用协议》约定的“延展至个推使其可以获取实现相关推送功能所必要的合理信息”中“相关推送功能”是否包括利用该 APP 共享链路而向其他 APP 最终用户发送通知，APP 最终用户是否知悉通过链路共享而向其发送其他 APP 通知，是否取得 APP 最终用户同意或授权；（2）抽样头部 APP 产品的《用户协议》、《隐私政策》中部分表述基于提升本 APP 服务之目的而收集用户数据并向第三方共享该数据，发行人链路共享是否属于“提升本 APP 服务之目的”。请保荐机构、律师发表核查意见。	8
二、信息披露问题:	12
问题 4:	12
请发行人在《招股说明书》中补充披露：（1）获取用户数据信息的来源、获取途径及授权方式，收集用户信息获得用户同意的具体制度及相关安排，收集用户信息时是否明确告知收集信息的范围及使用用途，对数据的使用是否超过必要的限度；（2）获取数据进行商业化变现的合规性；（3）在对用户信息进行加工、处理存储及传输过程中避免或防止泄露用户隐私的具体制度及相关安排；（4）用户信息保护技术体系，尤其是防止外部黑客攻击和内部人员恶意导致的数据泄露的技术措施；（5）最近三年发生的严重泄密事件、重大诉讼、处理结果及有关的整改措施；（6）通过公安部门信息系统安全等级保护测评的情况；（7）2018 年 5 月 25 日欧盟《通用数据保护条例》正式生效对发行人生产经营的影响及相关应对措施。请保荐机构、律师发表核查意见。	12

北京市万商天勤律师事务所

关于浙江每日互动网络科技股份有限公司

首次公开发行人民币普通股（A股）股票并在创业板上市 的补充法律意见书（十三）

致：浙江每日互动网络科技股份有限公司

本所依据与发行人签署的《法律服务合同》，担任发行人本次发行并上市的专项法律顾问。本所律师根据《公司法》、《证券法》、《创业板首发管理办法》、《从业管理办法》、《执业规则》等法律、法规和中国证监会的有关规定，按照中国证监会《编报规则第12号》的要求，遵照律师行业公认的业务标准、道德规范和勤勉尽责精神，对发行人已经提供的与本次发行有关的文件和事实进行了核查和验证，于2017年9月4日出具了《北京市万商天勤律师事务所关于浙江每日互动网络科技股份有限公司首次公开发行人民币普通股（A股）股票并在创业板上市的法律意见书》与《北京市万商天勤律师事务所关于浙江每日互动网络科技股份有限公司首次公开发行人民币普通股（A股）股票并在创业板上市的律师工作报告》，于2018年2月27日出具了《北京市万商天勤律师事务所关于浙江每日互动网络科技股份有限公司首次公开发行人民币普通股（A股）股票并在创业板上市的补充法律意见书（一）》，于2018年3月30日出具了《北京市万商天勤律师事务所关于浙江每日互动网络科技股份有限公司首次公开发行人民币普通股（A股）股票并在创业板上市的补充法律意见书（二）》及《北京市万商天勤律师事务所关于浙江每日互动网络科技股份有限公司首次公开发行人民币普通股（A股）股票并在创业板上市的补充法律意见书（三）》，于2018年7月2日出具了《北京市万商天勤律师事务所关于浙江每日互动网络科技股份有限公司首次公开发行人民币普通股（A股）股票并在创业板上市的补充法律意见书（四）》，于2018年8月20日出具了《北京市万商天勤律师事务所关于浙江每日互动网络科技股份有限公司首次公开发行人民币普通股（A股）股票并在创业板上市的补充法律意

见书（五）》、《北京市万商天勤律师事务所关于浙江每日互动网络科技股份有限公司首次公开发行人民币普通股（A股）股票并在创业板上市的补充法律意见书（六）》及《北京市万商天勤律师事务所关于浙江每日互动网络科技股份有限公司首次公开发行人民币普通股（A股）股票并在创业板上市的补充法律意见书（七）》，于2018年8月28日出具了《北京市万商天勤律师事务所关于浙江每日互动网络科技股份有限公司首次公开发行人民币普通股（A股）股票并在创业板上市的补充法律意见书（八）》，于2018年9月26日出具了《北京市万商天勤律师事务所关于浙江每日互动网络科技股份有限公司首次公开发行人民币普通股（A股）股票并在创业板上市的补充法律意见书（九）》、《北京市万商天勤律师事务所关于浙江每日互动网络科技股份有限公司首次公开发行人民币普通股（A股）股票并在创业板上市的补充法律意见书（十）》、《北京市万商天勤律师事务所关于浙江每日互动网络科技股份有限公司首次公开发行人民币普通股（A股）股票并在创业板上市的补充法律意见书（十一）》、《北京市万商天勤律师事务所关于浙江每日互动网络科技股份有限公司首次公开发行人民币普通股（A股）股票并在创业板上市的补充法律意见书（十二）》。

根据《证券法》、《公司法》、《编报规则第12号》、《从业管理办法》等法律、法规和规范性文件的有关规定，本着律师行业公认的业务标准、道德规范和勤勉尽责精神，遵照中国证监会的要求，就2018年10月30日中国证监会出具的《关于请做好浙江每日互动网络科技股份有限公司发审委会议准备工作的函》出具本补充法律意见书。

《法律意见书》、《律师工作报告》、《补充法律意见书（一）》、《补充法律意见书（二）》、《补充法律意见书（三）》、《补充法律意见书（五）》中释义适用于本补充法律意见书，本补充法律意见书构成对《法律意见书》、《律师工作报告》、《补充法律意见书（一）》、《补充法律意见书（二）》、《补充法律意见书（三）》、《补充法律意见书（四）》、《补充法律意见书（五）》、《补充法律意见书（六）》、《补充法律意见书（七）》、《补充法律意见书（八）》、《补充法律意见书（九）》、《补充法律意见书（十）》、《补充法律意见书（十一）》、《补充法律意见书（十二）》的补充，《法律意见书》、《律师工作报告》、《补充法律意见书（一）》、《补充法律意见书（二）》、《补充法律意

意见书（三）》、《补充法律意见书（四）》、《补充法律意见书（五）》、《补充法律意见书（六）》、《补充法律意见书（七）》、《补充法律意见书（八）》、《补充法律意见书（九）》、《补充法律意见书（十）》、《补充法律意见书（十一）》、《补充法律意见书（十二）》未被本补充法律意见书修改的内容继续有效。

本所律师根据有关法律、法规和规范性文件的规定，按照律师行业公认的业务标准、道德规范和勤勉尽责的精神，现出具补充法律意见书如下：

声 明

在出具本补充法律意见书之前，本所律师声明如下：

1、本所及本所律师依据《证券法》、《编报规则第12号》、《从业管理办法》和《执业规则》等规定及本补充法律意见书出具日以前已经发生或者存在的事实，严格履行了法定职责，遵循了勤勉尽责和诚实信用原则，进行了充分的核查验证，保证本补充法律意见书所认定的事实真实、准确、完整，所发表的结论性意见合法、准确，不存在虚假记载、误导性陈述或者重大遗漏，并承担相应法律责任。

2、发行人已书面承诺，其已向本所律师提供了出具法律意见书和律师工作报告所必需的全部有关事实材料、批准文件、证书和其他有关文件，有关材料无任何虚假记载、误导性陈述或重大遗漏，所有书面材料均真实、合法、有效，所有的复印件或副本均与原件或正本完全一致。

3、本所律师对与出具本补充法律意见书有关的事实、批准文件、证书和其他有关文件进行了核查，但本补充法律意见书仅就与本次发行并上市有关的中国境内法律问题发表法律意见，本所及本所律师并不具备对有关会计、验资及审计、资产评估及境外法律事项等专业事项发表专业意见的适当资格。本补充法律意见书中对有关会计报表、验资及审计报告、评估报告及境外法律事项等文件某些内容的引述，并不表明本所律师对该等内容的真实性、准确性、合法性作出任何判断或保证。

4、本补充法律意见书是本所律师基于对本次发行并上市有关事实的了解和对法律的理解而出具的。对于出具本补充法律意见书至关重要而无独立证据支持的证明的事实，本所律师依赖于有关政府部门、发行人或者其他有关单位出具的证明文件作出判断。

5、本所律师同意发行人在其为本次发行并上市编写的招股说明书中自行引用或按中国证监会审核要求引用本补充法律意见书的内容。但发行人作上述引用时，不得因引用而导致法律上的歧义或曲解。除本次发行并上市目的之外，非经本所同意，本补充法律意见书不得用于任何其他目的。

6、本所律师同意将本补充法律意见书作为本次发行并上市申报材料之一，随其他材料一起报送有关主管部门审核，并依法对发表的法律意见承担相应的法律责任。

正文

一、关注问题

问题 3:

请发行人说明并在《招股说明书》中补充披露：（1）与 APP 开发者《个推使用协议》约定的“延展至个推使其可以获取实现相关推送功能所必要的合理信息”中“相关推送功能”是否包括利用该 APP 共享链路而向其他 APP 最终用户发送通知，APP 最终用户是否知悉通过链路共享而向其发送其他 APP 通知，是否取得 APP 最终用户同意或授权；（2）抽样头部 APP 产品的《用户协议》、《隐私政策》中部分表述基于提升本 APP 服务之目的而收集用户数据并向第三方共享该数据，发行人链路共享是否属于“提升本 APP 服务之目的”。请保荐机构、律师发表核查意见。

回复:

（一）与 APP 开发者《个推使用协议》约定的“延展至个推使其可以获取实现相关推送功能所必要的合理信息”中“相关推送功能”是否包括利用该 APP 共享链路而向其他 APP 最终用户发送通知，APP 最终用户是否知悉通过链路共享而向其发送其他 APP 通知，是否取得 APP 最终用户同意或授权

公司与 APP 开发者就是否采用共享链接技术进行了明确约定，APP 最终用户选择同意接收信息通知，则意味着 APP 最终用户概括接受了公司通过任何技术方式向其完成信息推送，APP 最终用户无需知悉公司共享链路技术的具体运作方式，公司通过共享链路技术进行信息推送亦无需取得 APP 最终用户的单独同意或授权。相关具体论述如下：

1、公司与 APP 开发者之间就共享链路技术的授权和使用有清晰明确的约定

公司与 APP 开发者签署的《个推使用协议》等协议中明确约定，“APP 开发

者须以适当方式使用户知晓该 APP 产品集成了公司推送服务功能模块，并确保用户知悉且同意 APP 获取用户相关信息的权利适当延展至个推使其可以获取实现相关推送功能所必要的合理信息”。同时，公司在服务清单中明示，APP 开发者需对是否享受“共享链路”技术作出明确选择。若 APP 开发者不选择享受“共享链路”技术，则该 APP 的推送链路不会被其他 APP 使用，同时使用该 APP 的最终用户也不会因为“共享链路”技术而收到推送信息。若 APP 开发者选择享受“共享链路”技术，则公司将为其额外提供配置文档，该 APP 开发者需根据公司要求主动完成配置后，该 APP 方可以和其他同样选择享受“共享链路”技术的 APP 一样共享推送链路，而使用该些 APP 的最终用户可以接受到基于“共享链路”技术推送的信息。

共享链路技术是公司与 APP 开发者之间就提供推送服务过程中所采用的一种技术手段，是否享受共享链路技术是 APP 开发者的自由选择。

2、APP 开发者和最终用户之间就是否接受推送通知服务有清晰明确的约定

APP 最终用户在安装和首次使用 APP 时，APP 会弹出是否接收该 APP 的通知等选项，最终用户对此拥有自主选择权。在使用 APP 的过程中，最终用户随时可以根据自己的需求在移动终端设备中对是否接收该 APP 通知的权限进行调整。

APP 最终用户如果对接接收 APP 通知表示明示拒绝，则不会接收到该 APP 的通知信息；只有在其明示同意的情况下，APP 开发者才会向其发送信息（由公司提供信息推送技术服务）。APP 最终用户选择接收通知意味着其概括接受了公司通过任何技术方式向其完成信息推送工作，即 APP 最终用户并不需要知悉 APP 开发者所采用的具体推送技术。因此只要 APP 最终用户接受《用户服务协议》并同意接受 APP 的通知信息，则 APP 开发者就可以根据通知权限进行信息推送，而公司根据与 APP 开发者签署的《个推使用协议》的相关授权和约定，协助 APP 开发者完成其对最终用户的信息推送。

3、共享链路是信息推送过程中公司所运用的技术手段和方式，APP 最终用户无需知悉共享链路的具体运作方式，公司利用本 APP 通过共享链路技术向其他 APP 最终用户发送通知，并不需要额外获得本 APP 最终用户的授权

公司通过自身技术优势，为 APP 开发者提供一站式消息推送解决方案，将 APP 开发者的信息推送至最终用户。公司服务了数以万计的 APP，为每一个独立的 APP 都建立了从公司服务器到安装了该 APP 的移动终端之间“点对点”的连接链路。在移动终端中多个 APP 均存在“个推 SDK”的情况下，公司运用合并链路技术，将使用“个推 SDK”的 APP 之间的长连接链路进行合并，只要其中任何一个应用活跃，通过共享推送链路的方式，“个推 SDK”就可完成消息的下发推送。公司使用的合并链路技术实现了跨 APP 的链路共享，保持了应用进程的活跃度，有效保证了消息的下发展现。共享推送链路的方式减少了对运营商网络信令的浪费和对移动终端资源的消耗，达到了省电省流量的目的。共享链路技术是公司有别于其他推送服务方的显著技术优势和解决方案。

公司仅向明确同意享受“共享链路”技术的 APP 开发者提供该项技术服务。在运用共享链路技术的情况下，APP 的最终用户可能基于本 APP “点对点”的链路接收到本 APP 开发者推送的信息，也有可能基于其他 APP 的共享链路而接收到本 APP 开发者推送的信息，其他 APP 的最终用户也有可能基于本 APP 的共享链路而接收到彼 APP 开发者推送的信息。

链路共享只是一种提升信息推送效率的技术手段，不是信息共享，不会采集最终用户的个人信息，也不会对 APP 最终用户增加额外负担或义务，无论采取何种技术手段，APP 最终用户获取的信息不会因推送技术的差别而发生变化。因此 APP 最终用户无需知悉公司共享链路的具体运作方式，公司通过共享链路技术进行信息推送亦无需取得 APP 最终用户的单独同意或授权。

（二）抽样头部 APP 产品的《用户协议》、《隐私政策》中部分表述基于提升本 APP 服务之目的而收集用户数据并向第三方共享该数据，公司链路共享是否属于“提升本 APP 服务之目的”

公司在推送服务中使用链路共享技术，其目的是在确保推送信息有效触达 APP 最终用户的同时，还可以让移动终端省电省流量，最大限度的提升推送效率。链路共享技术不涉及收集用户数据信息，因此与为了“提升本 APP 服务之目的”

而收集用户数据并分享该数据有着本质的不同。具体论述如下：

1、APP 开发者为了更好的提供服务，收集用户数据后向包括公司在内的第三方共享该数据，公司获取用户信息后不会将其再共享给任何其他第三方

APP 开发者为了更好地向最终用户提供服务，引入第三方为其提供信息推送服务。为了实现推送的精准、高效，APP 开发者和提供推送服务的第三方需要收集用户信息（主要体现为 MEI/IDFA/MAC、机型、APP List、WiFi 信息等设备数据）。根据 APP 最终用户的授权和同意，APP 开发者将收集到的用户数据向包括公司在内的第三方共享，公司获取用户信息后用于信息推送服务，同时对上述用户信息进行加密、加工、处理，最终形成“个推大数据平台”的数据后进行商业化变现。此时，进行商业化变现的是由用户设备信息衍生出来的数据化产品而非用户个人信息。在上述信息获取、信息处理、平台数据商业化变现的全过程中公司不存在向任何第三方共享用户信息的情形。

2、公司收集用户信息是为了实现信息推送功能，共享链路是信息推送过程中所运用的技术方式，共享链路不存在收集用户信息、共享信息的情形

公司收集 APP 最终用户的具有唯一识别性的原始信息，其目的是为了实现在信息推送功能，将 APP 开发者的信息准确无误的推送至其最终用户。而共享链路技术的运用是为了提升推送效率而采用的科技创新方法。如前所述，在移动终端中多个 APP 均存在“个推 SDK”的情况下，公司运用合并链路技术，将使用“个推 SDK”的 APP 之间的长连接链路进行合并，只要其中任何一个应用活跃，通过共享推送链路的方式，“个推 SDK”就可完成消息的下发展示。共享链路技术的运用过程中不会收集用户信息，完成下发展示的信息是 APP 开发者要求公司推送的信息而不是用户信息，共享链路技术运用的整个环节中均不会产生用户信息共享给其他第三方的情形。

综上所述，共享链路技术的运用是为了确保消息下发展示的高效及准确，同时达到省电省流量的目的。而提升 APP 自身服务目的是为了“让用户获得更好的 APP 使用体验”。因此，共享链路等创新技术的运用与为了“提升本 APP 服务之目的”而收集用户数据并分享该数据有着本质的不同。

综上，本所律师认为：

1、发行人与 APP 开发者就是否采用共享链接技术进行了明确约定，APP 最终用户选择同意接收信息通知，则意味着 APP 最终用户概括接受了发行人通过任何技术方式向其完成信息推送，APP 最终用户无需知悉发行人共享链路技术的具体运作方式，发行人通过共享链路技术进行信息推送亦无需取得 APP 最终用户的单独同意或授权；

2、发行人在推送服务中使用链路共享技术，其目的是在确保推送信息有效触达 APP 最终用户的同时，还可以让移动终端省电省流量，最大限度的提升推送效率。链路共享技术不涉及收集用户数据信息，因此与为了“提升本 APP 服务之目的”而收集用户数据并分享该数据有着本质的不同。

二、信息披露问题：

问题 4：

请发行人在《招股说明书》中补充披露：（1）获取用户数据信息的来源、获取途径及授权方式，收集用户信息获得用户同意的具体制度及相关安排，收集用户信息时是否明确告知收集信息的范围及使用用途，对数据的使用是否超过必要的限度；（2）获取数据进行商业化变现的合规性；（3）在对用户信息进行加工、处理存储及传输过程中避免或防止泄露用户隐私的具体制度及相关安排；（4）用户信息保护技术体系，尤其是防止外部黑客攻击和内部人员恶意导致的数据泄露的技术措施；（5）最近三年发生的严重泄密事件、重大诉讼、处理结果及有关的整改措施；（6）通过公安部门信息系统安全等级保护测评的情况；（7）2018 年 5 月 25 日欧盟《通用数据保护条例》正式生效对发行人生产经营的影响及相关应对措施。请保荐机构、律师发表核查意见。

回复：

（一）获取用户数据信息的来源、获取途径及授权方式，收集用户信息获得用户同意的具体制度及相关安排，收集用户信息时是否明确告知收集信息的范围及使用用途，对数据的使用是否超过必要的限度

公司通过与 APP 开发者签署《个推使用协议》并经 APP 最终用户明示同意或授权而获取用户信息，APP 在《用户协议》中向终端用户明确告知了收集信息的范围及使用用途。公司对用户数据信息的使用符合个人信息收集的合法性要求、最小化要求及授权同意的要求，未超过必要限度。相关具体论述如下：

1、公司获取用户数据信息的来源、获取途径及授权方式，收集用户信息获得用户同意的具体制度及相关安排

（1）公司与 APP 开发者之间通过协议约定作为共同控制者获取用户数据信息

首先，公司与拟提供服务的 APP 开发者签署《个推使用协议》等书面协议，就公司获得用户数据信息的方式和范围进行约定。公司要求“APP 开发者须以适当方式使用户知晓该 APP 产品集成了公司推送服务功能模块，并应确保用户知悉且同意 APP 获取用户相关信息的权利适当延展至个推使其可以获取实现相关推送功能所必要的合理信息”。

其次，根据公司与 APP 开发者之间签署的《个推使用协议》等协议，APP 开发者将个推信息推送平台软件开发包（“个推 SDK”）嵌入 APP 软件，并授权公司通过 APP 软件获取推送所必需的合理用户信息。在 APP 开发者将“个推 SDK”与其移动应用集成后，公司可通过且仅通过集成了个推 SDK 的 APP 获取用户数据。

公司严格遵守《中华人民共和国网络安全法》、《电信和互联网用户个人信息保护规定》等规定，作为互联网信息服务提供者收集、使用 APP 用户个人信息的，通过 APP 开发者的客户服务等协议，明确告知用户收集、使用信息的目的、方式和范围，并根据双方的约定收集、使用信息。因此，APP 开发者通过《用户协议》、《隐私政策》等协议（统称“《用户协议》”）约定获得用户授权。

综上，公司系通过 APP 开发者获取用户数据信息，其获取的用户数据信息

来源于 APP 终端用户对 APP 开发者及经 APP 许可的第三方的同意和授权。

(2) 每日互动获取用户数据信息系根据协议约定在授权范围内获取

根据 APP 开发者与公司有关《个推使用协议》等协议就公司获得用户数据信息进行明确约定,“APP 开发者须以适当方式使用户知晓该 APP 产品集成了公司推送服务功能模块,并应确保用户知悉且同意 APP 获取用户相关信息的权利适当延展至个推使其可以获得实现相关推送功能所必要的合理信息”。

根据《中华人民共和国网络安全法》、《电信和互联网用户个人信息保护规定》等规定,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,并根据双方的约定收集、使用信息。因此,APP 开发者通过《用户协议》、《隐私政策》等协议(统称“《用户协议》”)约定获得用户授权。

(3) APP 开发者的用户协议明确了用户信息授权许可的范围及于第三方

根据核查 APP 开发者与用户之间的协议,公司合作的头部 APP 均在其用户协议中明确了用户知晓该 APP 产品集成了第三方的产品或服务,第三方有权基于用户对该 APP 的授权而获取用户信息,并在用户的授权范围内合法使用用户信息。

因此,公司不直接获取用户信息,而是通过 APP 开发者在获得终端用户授权后,通过 APP 开发者获得经用户授权的用户数据信息;而且,只有签署了《个推使用协议》同意上述约定的 APP 开发者,公司方通过其 APP 获得经用户授权的用户数据信息。公司不存在未经用户同意和授权获取信息的情形。

2、收集用户信息时是否明确告知收集信息的范围及使用用途,对数据的使用是否超过必要的限度

公司通过 APP 开发者向终端用户明示、公开收集用户数据信息用于优化用户 APP 的功能,并通过 APP 与终端用户协议获得终端用户的同意,符合合法、正当、必要的原则的信息收集及使用原则,不存在违反《网络安全法》、《电信和互联网用户个人信息保护规定》、《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》等规定的情形。

公司通过个推 SDK 采集用户如下信息：

(1) IMEI/IDFA/MAC 、机型等设备信息

由于国内大部分安卓手机上 Android ID 缺失,且存在大量非标准的小品牌手机所导致的 ID 重码现象,单一的手机设备信息无法准确对设备进行分辨,因此需获取 IMEI 等信息进行组合分析,以免设备重码,从而确定唯一设备 ID,用于进行个性化推送。

(2) 应用列表 (APP List)

公司采用合并链路技术进行技术推送。当一个设备有多个 APP 的推送链路同时活跃时,公司会通过投票机制动态决定让多条链路合并成一条链路,因此需获得移动终端的应用列表。合并链路可以达到省电省流量的目的。

(3) 网络信息

为了最大程度保持网络连接的稳定性,公司的推送 SDK 需要了解设备的网络状态,包括 WiFi、基站等网络信息连接状态,以保证最佳的心跳和联网策略,从而实现稳定连续的推送服务。

个推 SDK 采集的上述数据信息符合最少够用等原则。最少够用原则指除与个人信息主体另有约定外,只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。实际上,公司就其基础推送及互联网营销所采用数据,仅限于 MEI/IDFA/MAC、机型、APP List、WiFi 信息等设备数据,不存在收集 APP 用户个人信息等超范围获取额外数据等情形。

因此,公司通过 APP 开发者向终端用户明示、公开收集用户数据信息用于优化用户 APP 的功能,并通过 APP 与终端用户协议获得终端用户的同意,符合合法、正当、必要的信息收集及使用原则,不存在违反《网络安全法》、《电信和互联网用户个人信息保护规定》、《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》等规定的情形;公司通过 APP 终端用户授权后收集的该些个人常用设备信息系公司开展业务所必需的、合理的用户信息,并且上述用户信息仅用于 APP 要求的推送功能,属于 APP 通过终端用户授权同意的业务范畴内,符合个人信息收集的合法性要求、最小化要求及授权同意的要求,未超过必要限度。

（二）获取数据进行商业化变现的合规性

公司经授权合法获取用户信息后，对用户信息进行匿名化和去标识化处理，使其成为无法重新识别个人信息主体的平台大数据，公司将平台大数据用于互联网增值服务进行商业化变现，符合《电信和互联网用户个人信息保护规定》、《信息安全技术 个人信息安全规范》等相关法律、法规的要求，具体论述如下：

1、公司获取的信息不属于个人信息

公司用于推送业务所获得的 IMEI/IDFA/MAC、机型、APP List、WiFi 信息等用户数据信息并不属于《电信和互联网用户个人信息保护规定》（工业和信息化部令第 24 号）规定的：“电信业务经营者和互联网信息服务提供者在提供服务的过程中收集的用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码等能够单独或者与其他信息结合识别用户的信息以及用户使用服务的时间、地点等信息”等用户个人信息，亦不属于最高人民法院、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》（法释〔2017〕10 号）规定的：“电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等”公民个人信息。

2、公司获取用户信息后对其进行匿名化和去标识化处理

公司获取用户信息后经脱敏、筛选、清洗、整理，并经深度挖掘后建模，最终构建衍生出自己的“个推大数据平台”，具备独立的财产权属。公司个推大数据平台的数据为经过脱敏加密后的非用户信息，经过匿名化和去标识化处理后，其他方无法重新识别个人信息主体，该类数据已不属于个人信息的范畴。

根据《信息安全技术 个人信息安全规范》8.2 条之规定“共享、转让个人信息，应遵守以下要求：……b) 向个人信息主体告知共享、转让个人信息的目的、数据接收方的类型，并事先征得个人信息主体的授权同意。共享、转让经去标识化处理的个人信息，且确保数据接收方无法重新识别个人信息主体的除外。”，公司使用脱敏加密后的数据从事经营业务无需终端用户授权，因此也不会存在超越

用户授权许可范围的情形。

3、公司将处理后的数据信息用于商业化变现符合法律法规规定及与 APP 用户间的约定

（1）公司对“个推大数据平台”的数据享有独立的财产性权益

信息是数据的内容，数据是信息的形式。“个推大数据平台”数据产品中的数据内容虽然来源于原始用户信息，但经过公司的深度开发已不同于普通的网络数据。

公司经授权所获取的用户信息经脱敏、筛选、清洗、整理，并经深度挖掘、建模后形成衍生数据，该衍生数据经过了公司匿名化和去标识化处理，与网络用户信息、原始网络数据无直接对应关系。衍生数据经公司整合梳理成为适应市场需求的数据内容或大数据分析，并通过一定方式以商业化手段呈现给公司客户时，该等数据已经完全区别于初始用户信息，是具有价值的网络大数据产品。公司在合法获取用户信息的基础上，不断投入大量的智力劳动成果，因此公司对“个推大数据平台”的数据享有独立的财产性权益。

（2）公司将“个推大数据平台”的数据用于其他增值服务符合其与 APP 用户之间的约定

A. 轻推送、移动互动网营销服务

在 APP 开发者与公司签署的协议中，APP 用户已通过用户协议等方式授权公司向其推送信息，即在 APP 安装时明确提示用户是否同意向其推送消息，在同意情况下用户才会接收到消息推送，包括提醒类消息（微信通知等）、功能性消息（天气情况等）、商业性消息（淘宝、京东的促销广告信息，大众点评、美团的店铺活动信息）等，因此，公司向 APP 用户推送广告等信息未超越 APP 用户授权的范畴。

（2）用户画像、数据统计服务

用户画像、数据统计服务指公司为移动应用开发者提供的 APP 使用人群属性特征画像服务及使用人群数据统计服务，上述服务通过分析指定 APP 收集的数据为该 APP 开发者分析其用户的基本特征并出具分析报告。用户画像、数据

统计服务无需额外收集用户其他信息且分析报告多为用户某一特定类别的特征、趋势等，不会泄露特定个人信息，因此未超出用户协议授权范围，也未违反个人信息保护的法律规定。

（3）其他数据服务

公司其他数据服务主要为 DMP（Data Management Platform）业务，即把分散的多方数据进行整合纳入统一的技术平台，并对数据进行标准化和细分后形成数据管理平台。公司通过技术推送等服务所积累的海量数据，经脱敏、挖掘、整合后形成了具有标签化、精细化特征的“数据仓库”，可以帮助客户识别虚假流量，指导其在程序化广告的采买中进行交易。公司提供上述服务无需另行采集用户信息，也无需向任何第三方透漏用户数据信息，仅需通过客户提供的信息为客户提供价值判断，因此未超出用户协议授权范围，也未违反个人信息保护的法律规定。

（三）在对用户信息进行加工、处理存储及传输过程中避免或防止泄露用户隐私的具体制度及相关安排

1、公司对于用户信息加工的过程及其对用户隐私的保护安排

公司对收集到的具有唯一识别性的原始数据（例如 IMEI）使用 MD5 加密、自定义用户标识、用户特性模糊化标签化、数据使用群体化等技术手段使其脱敏，脱敏后的数据无法单独或者与其他信息结合识别至特定个人且不能复原。公司通过对数据脱敏、筛选、清洗、整理，并经深度挖掘后建模，最终构建出自己的“个推大数据平台”。

个推大数据平台的具体形成过程及其对用户隐私的保护安排如下：

（1）数据处理

在数据处理过程中，公司对于获取的数据进行脱敏转换加密处理后，通过算法生产匿名的推送 CID，实现数据的完全脱敏。该种去标识化的处理已经将“个推大数据平台”的数据与用户个人信息明显区分开来。服务器对上述脱敏数据进行脏数据清洗、数据格式转换、加密和存储后，变成中间层数据存储到数据仓库

中。

（2）数据建模

公司对中间层数据进行建模处理，建模处理后对不同的数据加上特定标签，公司最终将带有标签的数据汇总至个推大数据平台，用于公司其他数据增值服务。

综上，进入到个推大数据平台中的数据信息为脱敏加密后的标签数据，在整个数据的处理过程中，可实现对获取数据的保密且不可逆，也最大限度的对用户隐私进行了保护。

2、公司对于用户信息处理存储及传输过程中的防护措施

为保证数据资产安全、保障用户合法权益，公司制定了《个推数据安全保障技术实施指南》、《个推对外数据安全管理制度》等规定。其中对于用户信息处理存储及传输过程中的防护措施主要包括：

（1）采集环节

A. 防火墙策略。即在正常业务中，服务仅允许指定的 IP 来访问。

B. 认证鉴权。数据采集时需要根据采集方法的不同进行不同方式认证鉴权，可通过账号密码、随机短信、动态口令等方式认证服务来实现用户身份的验证，并通过限制采集系统的 IP 地址，端口号等方式确保合规的 IP 和端口进行数据采集工作。

C. 日志采集及异常告警。对采集行为进行日志记录，记录的日志内容包括采集行为详细的操作日志和执行日志，如出现异常采集行为及时告警。

（2）传输环节

A. 通道加密。数据采集时对传输通道进行加密，采用可靠的传输方式。

B. 敏感数据加密。对敏感性数据本身用安全的加密算法加密，确保数据的机密性。

C. 完整性校验。采用完整性校验算法，确保数据的完整性和可用性。

D. 启用 SSL（Secure Sockets Layer 安全套接层）。

（3）存储环节

A. 数据封装。数据封装能够尽可能屏蔽内部的具体细节，避免受到外界的干扰和误用，从而确保了安全。数据封装主要有两种方法：a.依据面向对象编程中的概念，把数据和操作数据的函数捆绑封装；b. 封装数据库，避免内部系统或者外部系统都直接访问源数据库，或者在遭受攻击时数据库服务器信息直接泄露。

B. 备份及恢复。大数据平台自身具备三备份功能，特别需要对集群中主节点（HDFS）的 HA 功能进行设置与配置，保证数据存储层的高可用性，同时还应该提供完备的数据备份和恢复机制来保障数据的可用性和完整性。

（四）用户信息保护技术体系，尤其是防止外部黑客攻击和内部人员恶意导致的数据泄露的技术措施

1、用户信息保护体系

根据敏感程度和商业价值不同，公司将数据划分为三级：高敏感级、中敏感级、低敏感级。各级数据的基本管控要求如下：

（1）高敏感级数据基本管控要求

对高敏感级数据应实施较严格的技术和管理措施，保护数据的机密性和完整性，确保数据访问控制安全，建立数据安全规范以及数据准实时监控机制。高敏感级数据在满足相关条件的前提下，可以对外开放。

A. 禁止对外提供高敏感级原始数据，但有单独规定的除外；

B. 在高敏感级数据中，客户密码及关联信息的原始信息经过客户相关书面申请、通过相应业务主管初审以及至少 3 名数据委员会成员审核后，方可对客户提供；

C. 对外的系统账号和密码的原始信息，通过相应业务主管初审以及至少 2 名数据委员会成员审核后，方可向客户提供；

D. 网络身份标识、客户行为的标签数据、服务内容数据、服务记录和日志

的标签数据、群体数据，通过相应业务主管初审以及至少 3 名数据委员会成员审核后，方可对外提供。超过 1 万条时，还需要通过 CEO 审核；

E. 设备连接数据，设备行为数据，必须经过脱敏处理，通过相应业务主管初审和至少 3 名数据委员会成员审核后，方可对外提供。超过 1 万条时，还需要通过 CEO 审核。

（2）中敏感级数据基本管控要求

对中敏感级数据应实施必要的技术和管理措施，确保数据生命周期安全，建立数据安全管理制度。中敏感级数据在满足相关条件的前提下，可以对外开放。

A. 移动终端设备资料的群体数据和标签数据，通过相应业务主管初审和至少 2 名数据委员会成员审核后，方可对外提供。超过 1 万条时，还需要通过 CEO 审核；

B. 对外服务 IP，通过相应业务主管初审和 CTO 审核后，方可对外提供。

（3）低敏感级数据基本管控要求

对低敏感级数据应实施基本的技术和管理措施，确保数据生命周期安全。低敏感级数据可以直接对外开放，但需要考虑对外开放的数据量及类别，避免由于类别较多或者数据量过大，导致能够用于关联分析。其中：

A. 客户业务订购关系的群体数据、标签数据，通过相应业务主管初审和至少 1 名数据委员会成员审核后，方可对外提供；

B. 面向客户的公司 WIFI 密码必须 3 个月修改一次，且密码至少 6 位，包含数字和字母。

2、防止外部黑客攻击和内部人员恶意导致的数据泄露的技术措施

（1）网络隔离

与合作方的相关业务数据属于生产数据，位于生产环境网络。禁止办公网络、公网直接访问，必须通过 VPN。对于相关业务人员的 VPN 的开通，必须经过公司严格的审批流程。

数据使用者必须严格遵守安全基线配置规定。同时公司仅开放了合作方业务

数据所涉及的端口和映射，并关闭不必要的端口和服务。

数据使用者必须通过堡垒机才能访问经过授权的生产环境的主机。公司仅向相关技术人员提供堡垒机账号权限，且账号及其权限必须经过严格的流程审批。

（2）漏洞扫描

安全部门定期（一般每隔 3 个月）对生产环境主机和应用进行安全漏洞扫描，形成完整的安全报告（内容包含要求修复的漏洞及推荐方案），提交公司安全委员会审阅，并且与合作方的业务团队必须开展后续安全漏洞修复工作，以增强主机和应用的安全性。

（3）安全测试

针对合作方业务相关的应用，每次由安全部门在测试阶段按照安全基线要求进行安全测试。根据结果通过与否，决定能否上线。如果需要强制上线，则需要经过公司安全委员会成员同意，并采取必要的漏洞危害缓解措施。

（4）服务监控

当网络、应用出现异常时，需采用自动安全保障系统，通过短信、微信或者邮件的方式第一时间通知相关技术人员及主管，确认并修复故障，以确保服务的可用性和稳定性，并于第一时间，将故障原因及修复情况告知客户。

（5）电子流程审批及审计

为了加强数据安全保障，制定相关电子审批流程，加强内部安全控制。凡是涉及网络权限、主机权限、数据访问权限等操作都要求执行电子审批流程。

安全部门会定期（每隔 3 个月）对全部流程进行安全审计，提交审计报告给安全委员会。并就审计出的问题要求相关部门进行整改，必要时，采取相应的惩罚措施。

安全部门同时根据业务的发展，及时优化或者新增必要的审批环节。

（6）安全培训

安全部门定期（每隔 3 个月）针对合作方业务系统相关的产品设计、技术人员组织专题安全培训，从 SDL 流程上加强应用的安全保障。

安全部门针对公司全体成员，组织不定期的安全讲座，宣传公司的安全制度规范，针对新人入职进行安全培训，从员工入职第一天开始增强员工安全意识。

（7）安全制度规范

公司全体员工必须严格遵守《个推安全管理细则》、《个推对外数据安全管理制度》、《数据库管理及制度》等一系列安全管理规定，由业务内控部进行监督执行。

同时，定期根据公司实际情况，由业务内控部对相关的安全规定进行审查和调整，提交公司安全委员会审核后，由行政部面向全体员工发布。

（五）最近三年发生的严重泄密事件、重大诉讼、处理结果及有关的整改措施

公司已取得杭州市公安局网络警察分局出具的证明文件，证明公司自 2010 年 12 月 7 日至 2018 年 6 月 30 日，未发现公司存在违反互联网信息管理有关法律、法规和规范性文件的情形，无与互联网信息服务管理有关的行政或刑事处罚记录。

根据公司的说明，中介机构通过公开信息及“国家企业信用信息公示系统”、“中国裁判文书网”、“中国执行信息公开网”、“全国法院被执行人信息查询系统”、“信用中国”、“浙江法院公开网”等系统及仲裁机构网站查询，截至目前，公司不存在个人信息、隐私泄露事件，且公司系通过 APP 开发者经用户授权后在 APP 开发者共同控制情况下收集、使用其业务所需的用户常用设备识别信息等用户个人信息，不涉及用户个人隐私及敏感信息，不存在侵权风险，亦存在纠纷或潜在纠纷。

（六）通过公安部门信息系统安全等级保护测评的情况

1、国家信息安全等级保护的重要性

信息安全等级保护是我国信息安全保障的一项基本制度，作为信息安全系统分级分类保护的一项国家标准，对于完善信息安全法规和标准体系，提高安全建

设的整体水平，增强信息系统安全保护的整体性、针对性和时效性具有重要意义。

信息安全等级保护包括定级、备案、安全建设和整改、信息安全等级测评、信息安全检查五个阶段，要求不同安全等级的信息系统应具有不同的安全保护能力。信息安全保护等级共分为 5 级，等级越高，意味着安全保护能力越强。

根据《信息安全等级保护管理办法》规定，信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。经查询公开信息，浪潮信息（000977）、三六零（601360）、阿里云计算有限公司、广州网易计算机系统有限公司等公司的信息系统被评定为等级保护第 3 级。

2、公司的信息安全系统保护等级认证过程

浙江东安检测技术有限公司¹于 2017 年 8 月 24 日至 2017 年 10 月 20 日期间对公司的个推推送业务系统开展了信息安全等级保护测评工作。测评过程包括测评准备、方案编制、现场测评及分析与报告编制。测评范围包括物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复、安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运营管理等方进行安全测评。

经详细测评后，浙江东安检测技术有限公司出具了《个推推送业务系统安全等级保护定级报告》并认定，个推推送业务系统信息遭到破坏后，所侵害的客体是公民、法人和其他组织的合法权益，同时也侵害社会秩序和公共利益，根据信息受到破坏时所侵害的客体以及侵害程度，个推推送业务系统业务信息安全保护等级为第三级。

根据《信息安全等级保护管理办法》，信息系统的安全保护等级分为五级，其中需要第三级保护的系统标准为：信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。第三级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护，国家信息安全监管部门对该级信息系统信息安全等级保护工作进行监督、检查。

¹ 浙江东安检测技术有限公司是国家公安部授权的专业的第三方测评机构，是公安部通报中心技术支持单位，也是全国第一批从事网络安全等级保护工作的测评机构。

3、公司信息安全系统保护等级认证备案结果

2017 年 12 月 29 日，公司通过信息系统安全等级保护测评，取得杭州市公安局核发的《信息系统安全等级保护备案证明》，备案项目为第三级个推推送业务系统，即个推推送业务系统符合信息系统安全等级保护第 3 级（S3A2G3）保护要求。根据国家信息安全等级保护的相关政策要求，第三级是指信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。公司个推推送业务系统获得等级保护第 3 级证明充分说明了公司信息系统及信息数据具有相当的重要性，同时也证明了公司对信息系统的安全保护能力达到了较高的水平。

（七）2018 年 5 月 25 日欧盟《通用数据保护条例》正式生效对发行人生产经营的影响及相关应对措施

1、欧盟《通用数据保护条例》的适用范围

《通用数据保护法案》（General Data Protection Regulation, GDPR）于 2018 年 5 月 25 日起正式施行，旨在加强欧盟境内居民的个人数据和隐私保护，该法案保护对象及管辖范围主要如下：

（1）保护对象

GDPR 保护的對象为“个人数据”，不涉及除个人数据以外的其他数据。

根据 GDPR 第 4 条的规定，个人数据是指任何指向一个已识别或可识别的自然人（数据主体）的信息。可识别的自然人信息是指可以通过参照如姓名、身份证号码、定位数据、在线识别信息等，或通过一个或多个具体的物理的、生理的、基因的、精神的、经济的、文化的或社会的特征，直接或间接的识别自然人的信息。

（2）管辖范围

GDPR 第 3 条规定，除了适用于在欧盟内部设立的数据控制者或处理者对个人数据的处理（不论其实际数据处理行为是否在欧盟内进行外），如果存在以下

几种情况，即使控制者和处理者没有设立在欧盟内，GDPR 同样适用于其对欧盟内的数据主体的个人数据处理：

A. 向欧盟境内数据主体提供商品和服务的（不论该商品或服务是否需要支付对价）；

B. 监控数据主体在欧盟境内行为的；

C. 对个人数据的处理由欧盟外控制者进行，但根据欧盟成员国法律可以通过国际公法适用于该控制者所在地的。

2、公司对于《通用数据保护条例》的应对措施及受到的影响

（1）GDPR 施行后，公司的应对措施

自 GDPR 发布后，公司在积极熟悉法案的基础上，相应调整了境外业务拓展策略。

一方面，根据公司提供的信息及业务拓展情况，公司在报告期内未与任何欧盟地区客户签署服务协议，公司已通过 IP 设别等技术手段最大限度过滤来自欧盟地区的终端设备，一旦终端设备被判定为来自欧盟地区，则公司不会收集该终端设备数据，从而避免了获取来自 GDPR 管辖范围内的个人数据。

另一方面，为帮助部分 APP 开发者满足其在欧盟地区业务开展的要求，公司对该部分业务拓展有需求的 APP 开发者有针对性的研发出“欧盟地区适用的专用版 SDK”，该版本的 SDK 仅实现最基本的推送功能，同时不收集任何终端设备数据，主动规避 GDPR 监管风险。

（2）公司的未来经营活动不会受到 GDPR 的实质性影响

自 GDPR 发布后，公司在积极熟悉法案的基础上，不断审视和完善自身内部控制制度。对于基础推送类需要采集终端用户信息的服务进行了调整，通过识别终端 IP 地址的方式判断设备及用户来源，对于出自欧盟范围内的终端数据不做采集，主动规避 GDPR 监管风险。公司一贯对于信息的采集和使用严格遵守相关法律法规要求，并定期对潜在风险进行评估。GDPR 实施后，公司主动与相关 APP 开发者，以及工信部、司法审判机关等相关权威机构保持沟通，以便就个人数据收集、使用、存储、监管等政策法规的监管和应对做到合法合规。

根据普华永道出具的《信息科技控制评估和数据分析报告》，通过解析 IP 地址后对地域分布情况进行统计，公司日活跃设备中欧盟地区的活跃设备量占比较低，平均占比仅为 0.53%，均未超过 1%。若公司未来在境外加深拓展经营活动的，公司将严格按照 GDPR 相关要求适时调整在欧盟地区的经营策略以确保相关经营活动满足 GDPR 的要求。

因此，GDPR 的施行，对公司未来经营活动不存在实质性影响。

综上，本所律师认为：

1、根据发行人与 APP 开发者之间签署的《个推使用协议》等协议，APP 开发者将个推信息推送平台软件开发包整合进 APP 软件并授权发行人获取推送所必需的合理用户信息。因此，发行人系通过 APP 开发者获取用户数据信息并已取得用户的同意。发行人通过 APP 开发者向终端用户明示、公开收集用户数据信息用于优化用户 APP 的功能，并通过 APP 与终端用户协议获得终端用户的同意，符合合法、正当、必要的原则的信息收集及使用原则，对数据的使用未超过必要限度；

2、发行人获取的用户信息不属于用户个人信息，发行人获取上述数据后经脱敏、筛选、清洗、整理，并经深度挖掘后建模，最终构建衍生出自己的“个推大数据平台”，具备独立的财产权属，发行人将个推大数据平台的数据产品进行商业化变现不违反法律法规规定；

3、发行人为保证数据资产安全、保障用户合法权益，制定了《个推数据安全保障技术实施指南》、《个推对外数据安全管理规定》等规定，保障用户信息进行加工、处理存储及传输过程中安全性；

4、根据敏感程度和商业价值不同，发行人将数据划分为三级，采取不同的要求进行管控，同时采用网络隔离、服务监控等技术手段保证数据安全；

5、经查询，发行人最近三年未发生的严重泄密事件、重大诉讼；

6、经浙江东安检测技术有限公司现场的信息安全等级保护测评，发行人满足信息安全保护等级为第三级的要求，并已于 2017 年 12 月 29 日，发行人通过信息系统安全等级保护测评，取得杭州市公安局核发的《信息系统安全等级保护

备案证明》；

7、发行人不在欧盟 GDPR 管辖范围内开展业务，GDPR 的施行对发行人未来经营活动不存在重大实质性影响。

（此页无正文，专用于《北京市万商天勤律师事务所关于浙江每日互动网络科技有限公司首次公开发行人民币普通股（A股）股票并在创业板上市的补充法律意见书（十三）》的签署）

北京市万商天勤律师事务所



负责人：李宏 律师

经办律师：吴卿 律师

（签名）

（签名）

周游 律师

（签名）

徐璐 律师

（签名）

2018年10月31日