“知情同意”还能解决一切问题吗?

作者：杨迅 | 杨坚琪

无论过去还是现在,“知情同意”都不能解决所有的问题。

“知情同意”原则赋予信息主体对于其个人信息的控制权利，在个人信息处理中扮演着重要的角色。在实践中，“知情同意”往往亦是信息处理者收集、使用、储存个人信息的必要条件，也是《隐私政策》或者《个人信息保护声明》存在的核心作用。这就造成一个误解：似乎只要用户点击同意一份《隐私政策》或者《个人信息保护声明》，对用户个人信息的处理就具有合法性和正当性；更有观点认为，无论《个人信息保护声明》如何起草，只要本人同意，个人信息处理者就可以对个人信息“为所欲为”。但是中国法律真是这样要求的吗?

主要法律的留白

中国法下对于个人信息保护的规定渊远流长。早在 2012 年全国人大常委会发布的《关于加强网络信息保护的决定》中，就要求网络服务提供者和其他企业事业单位在“收集、使用公民个人电子信息”时，需要满足“明示收集、使用信息的目的、方式和范围，并经被收集者同意”的要求。这应是中国法律首次对个人信息保护提出原则性要求，且该等要求不断被后续的法律所延续。例如，2013 年修订的《消费者权益保护法》第 29 条规定“经营者收集、使用消费者个人信息，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，并经消费者同意”；2016 年颁布的《网络安全法》第 41 条规定，网络运营者“收集、使用”个人信息，应当“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”；而 2021 年 1 月 1 日生效的《民法典》第 1035 条则同样提出了“公开处理信息的规则”、“明示处理信息的目的、方式和范围”以及“征得该自然人或者其监护

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

人同意”的要求。**将上述法律下的个人信息保护规则进行归纳，我们认为核心要求为两点：1) 公示规则；以及 2) 获取用户对于规则的同意，即目前业界常说的“知情同意”原则。**

但是上述主要的法律规范均未对“知情同意”原则如何落地进行详细解释，也未明确是否满足“知情同意”原则即可处理个人信息。即使存在《信息安全技术-公用系统和商用系统个人信息保护指南》《信息技术安全-个人信息安全规范》等推荐性标准或者指南辅助解释，但是囿于法律效力的限制，上述规范或者指南的规定并不具有强制执行力，这使得实践中对于满足“知情同意”要求是否等于“可以处理个人信息”这类问题没有准确的答案。从这个意义上而言，主要的法律规定仅仅提出了“知情同意”要求，却对其能否单独作为处理个人信息的合法依据存在“留白”之处。

《个人信息保护法》目前正处于二次征求公众意见的阶段，因此目前中国仍然缺少一部统一的个人信息保护法律。而如前所述，主要法律的留白导致在实践中，不少企业以为只要通过《个人信息保护声明》获得个人信息主体同意即可满足个人信息保护的要求。另一方面，亦有法律从业者对个人信息保护的关注重点留存于简单的文件审核工作。上述观点均忽略了一个重要的事实：在不断积累经验之后，监管部门对个人信息处理的要求早已超出了形式意义上的“知情同意”原则。

《必要个人信息范围规定》的冲击

已经于 2021 年 5 月 1 日生效的《常见类型移动互联网应用程序必要个人信息范围规定》(**“《必要个人信息范围规定》”**)总结了网信办为首的主管部门近年来的监管经验，同时也反映了监管部门对进一步揭开“知情同意”模式面纱的勇气和决心。在《必要个人信息范围规定》正式颁布之前，带有官方色彩的公众号“App 个人信息举报”曾于 2020 年 11 月 2 日至 2020 年 11 月 23 日期间内发起系列投票，对 38 类服务的“最小必要个人信息”范围公开征求意见。从这个角度而言，《必要个人信息范围规定》在制定时也充分考虑了公众意见。

虽然《必要个人信息范围规定》全文仅短短七条，但其第三条的规定，“***App 不得因为用户不同意提供非必要个人信息，而拒绝用户使用其基本功能服务***”，则在“知情同意”要求之外施加了实质性的法律义务，并且对现有 App 的运营模式产生巨大的影响。依据第三条的规定，5 月 1 日后，以下几种常见的 App 运营模式的合法性都存在疑问：

- 仅在《个人信息保护声明》中列举需要收集的个人信息，并未区分“基本业务功能”和“拓展业务功能”及其对应所需的个人信息范围
- 用户一旦不同意《个人信息保护声明》，即不允许用户使用该等 App
- 在 App 更新版本后，若用户不同意更新后的《个人信息保护声明》，则不允许用户使用更新后的 App
- 在用户同意《个人信息保护声明》后，“打包”开启用户权限(尤其是个人敏感信息)，但并未区分用户权限的类型
- 在用户同意《个人信息保护声明》后，未向用户提供控制其“非必要个人信息”收集、使用方式的途径

而除了上述对于 App 运营者需要考虑的 App 业务逻辑变更之外，《必要个人信息范围规定》的出台也再次确认了简单的“知情同意”模式无法满足监管部门对于个人信息保护提出的法律要求。为何是“再次”?因为实际上，在主要法律之外，各个部门的立法实践早已对“知情同意”模式提出了更高的要求。

单行监管要求

近些年来，随着侵犯个人信息权益事件的不断曝光，除网信办、公安部之外，工信部、人民银行、证监会等行业主管部门都认识到单纯的“知情同意”要求并不能有效实现保护个人信息的目的。因此，根据行业或者业务的特点，在“知情同意”之外，各行业主管部门陆续出台了适用于其行业的额外保护规则:

1. **电信业务(例如通过 App、小程序开展业务和提供服务)**
   - 电信业务服务提供者应说明提供查询、更正信息的渠道
   - 不得收集其提供服务所必需以外的用户个人信息
   - 不得将信息用于提供服务之外的目的
   - 不得默认配置选择同意隐私政策
   - 未经用户同意之前，不得收集用户信息或者申请打开权限
   - 在申请打开可收集个人信息的权限，或者申请收集个人敏感信息时，未能告知用户目的

2. **金融业务**
   - 不得收集与业务无关的消费者金融信息
   - 不得采取不正当方式收集消费金融信息
   - 不得变相强制收集消费者金融信息
   - 不得因金融消费者不同意处理其金融信息为由绝提供金融产品或者服务，但必要的金融消费者信息除外
   - 为营销、调查和改进体验目的收集消费者金融信息的，应当给与金融消费者自主决定的权利，且不得因消费者不同意而拒绝向其提供金融产品或者服务

3. **电子商务**
   - 禁止使用概括授权、默认授权、捆绑授权、停止安装使用的方式，收集、使用与经营活动无直接关系的信息
   - 收集、使用个人生物特征、医疗健康、金融账户、个人行踪等敏感信息的，应当逐项取得消费者同意
   - 除非经法律要求或者被收集者授权同意，不得向包括关联方在内的任何第三方提供消费者信息

4. **医药健康**
   - 采集人口健康信息，应当遵循“一数一源、最少够用”的原则
   - 采集人类遗传资源，应当告知采集目的、采集用途、对健康可能产生的影响、个人隐私保护措施及其享有的自愿参与和随时无条件退出的权利

- 除医务人员和医疗行政管理部门以外，任何机构或个人均不得查阅患者病历(以及电子病历)

而 2021 年 4 月 27 日公布的**《移动互联网应用程序个人信息保护管理暂行规定(征)》**，更是对 App 运营者新增了一系列在"知情同意"之外的要求，例如:

- 动态申请 App 所需权限，不得强制通过一揽子授权方式申请打开多个系统权限;
- 处理个人信息的数量、频次和精度应当为服务所必须;
- 个人信息的本地读取、写入、删除、修改等操作应当为服务所必需，不得超出用户同意的操作范围。

我们理解上述规定其实曾在《App 违法违规收集使用个人信息自评估指南》以及《网络安全标准实践指南—移动互联网应用程序(App)收集使用个人信息自评估指南》等出现过类似的要求，因此本次的征求意见稿实质上是将监管经验升级为部门规章，从而使其具有法律效力。在另一方面，这也表示 App 运营者有必要关注主管部门平时发布的指南或者指导，因为其中的要求或许在未来会变成正式的法律要求。

除了上述行业规定之外，在司法实践中，亦有法院在司法裁决中不断对通过"知情同意"模式概括收集的用户个人信息的合理使用边界进行探索。例如，在 2020 年 8 月的"微信读书案"[(2019)京 0491 民初 16142 号]中，法院认可腾讯公司在《微信读书软件许可及服务协议》确实载明微信好友可以相互查看读书信息，但是《微信读书软件许可及服务协议》存在"透明度"不足的问题，因此其向用户的"告知"并不充分，由此得出未能获得用户的对于公开其"读书数据"的有效同意的结论，违反适时生效的法律规定。

《二审稿》下的最新动向

备受瞩目的《个人信息保护法(草案二审稿)》(**"《二审稿》"**)于 2021 年 4 月 30 日发布并向全社会公开征求意见。作为个人信息保护领域的首部综合性法律，《个人信息保护法》对"知情同意"规定的具体落实作出规定。不出意外地，在延续《个人信息保护法(草案一审稿)》(**"《一审稿》"**)的基础上，针对处理个人信息，《二审稿》在"知情同意"要求外新增了如下限制:

- 最小必要: 《二审稿》的第 6 条进一步明确了"最小必要"要求。与《必要个人信息范围规定》规定的类似，《二审稿》要求处理个人信息应当限定在"实现处理目的所必要的最小范围"内，也不得处理与处理目的无关的信息。同时，应当**采取对个人信息影响最小的方式**。

  根据第 6 条的规定，处理个人信息不仅需要遵守"知情同意"规定，同样会受到"最小必要"要求的约束，这对于希望通过一份"包罗万象"的《个人信息保护政策》或者《隐私政策》笼统地获取用户同意并以此为基础收集个人信息的企业而言，无疑是一个噩耗。**"最小必要"要求企业必须审核自身提供的服务与处理信息之间的关联性，而无法仅仅通过一纸政策为自身的行为免责。**

- 单独同意: 《一审稿》提出了一个新的概念-"单独同意"，《二审稿》仍然延续了该等要求。即，在某些信息主体权益影响较大的场景时，个人信息处理者应当在处理前，获取用户的"单独同意"，这

些场景包括: 向第三方提供处理后的信息、公开个人信息、处理敏感个人信息、向境外提供个人信息等。

无论最终立法者如何要求实现“单独同意”, 我们理解只要该等规定在最后的生效稿中仍然存在, 即意味着通过一揽子打包形式获取用户同意的“知情同意”模式可能无法符合法律要求。

虽然《个人信息保护法》仍然未能正式生效, 但是通过梳理《一审稿》和《二审稿》的变化, 仍然可以得出立法者对**仅以“知情同意”作为处理个人信息的理由持否认立场**。因此, 在《个人信息保护法》生效后, 单纯的一纸《隐私政策》(无论其内容多么完善)将更加无法满足法律和监管部门的要求。

建议

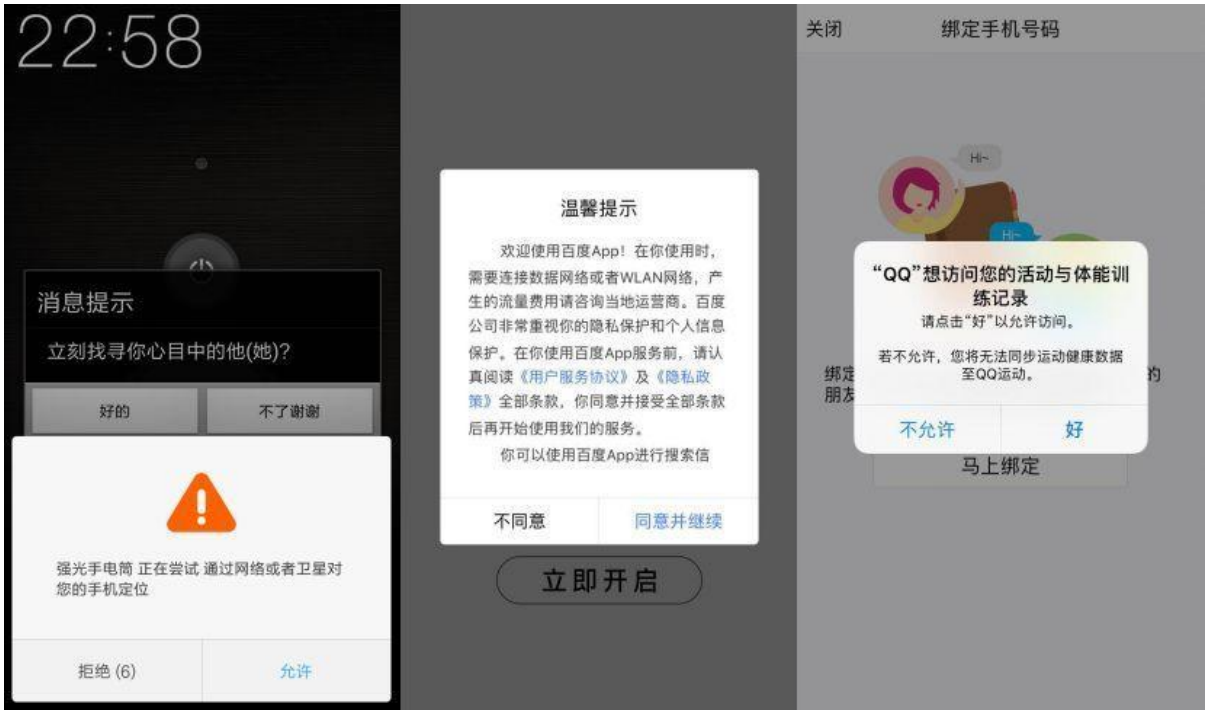
随着《必要个人信息范围规定》和《网络交易监督管理办法》在 5 月 1 日起的正式生效, App 运营者有必要重新审视目前使用的《隐私政策》以及收集、使用个人信息的实践是否符合法律要求。我们认为尤其需要关注的方面有:

- 确认 App 的“基本业务功能”(可能存在多个)以及对应的“必要个人信息”
- 评估业务逻辑, 调整弹窗界面和跳出时机
- 修订《隐私政策》/《个人信息保护政策》
- 进行代码审计, 确认目前收集个人信息的范围与《隐私政策》中列明的一致(尤其是通过系统函数接口和通过代码库复制的代码收集个人信息的范围)

很显然的一点是, 《必要个人信息范围规定》仅仅是撕开“知情同意”形式合规面纱的一个前兆, 即将出台的《个人信息保护法》必然会对个人信息处理提出更全面的规范要求。而对“知情同意解决一切”的命题, 则从来都只是一个美好幻想。

文末小问题:

5 月 1 日之后, 以下 App 中授权机制的展示方式, 是否仍然符合中国法律要求?


22:58
消息提示
立刻找寻你心目中的他(她)?
好的
不了谢谢
强光手电筒 正在尝试 通过网络或者卫星对您的手机定位
拒绝 (6)
允许
温馨提示
欢迎使用百度App！在你使用时，需要连接数据网络或者WLAN网络，产生的流量费用请咨询当地运营商。百度公司非常重视你的隐私保护和个人信息保护。在你使用百度App服务前，请认真阅读《用户服务协议》及《隐私政策》全部条款，你同意并接受全部条款后再开始使用我们的服务。
你可以使用百度App进行搜索信
不同意
同意并继续
立即开启
关闭
绑定手机号码
"QQ"想访问您的活动与体能训练记录
请点击"好"以允许访问。
若不允许，您将无法同步运动健康数据至QQ运动。
不允许
好
马上绑定

如您希望就相关问题进一步交流，请联系：

杨 迅
+86 21 3135 8799
xun.yang@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市建国门北大街 8 号 华润大厦 4 楼 T: +86 10 8519 2266 F: +86 10 8519 2929	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野