NEWSLETTER 数据合规

2020 第二期 /总第十五期

数据合规时事速递

北京市环球律师事务所

2020 年 1 月 23 日

目录

前 言

随着《网络安全法》及相关配套法律法规等文件的出台，中国正日益加强对个人信息安全的保护和对网络安全监管。我国对个人信息保护和网络数据安全越来越重视，监管趋势也越来越严。

环球律师事务所数据合规团队收集了国内外最新出台的重要法律法规、市场监管动向以及相关处罚案例，旨在为本期刊的读者提供最实时的法律动态，帮助读者第一时间了解网络治理、信息安全相关信息。帮助客户迎接数据时代的机遇与挑战。

环球律师事务所
GLOBAL LAW OFFICE

团队介绍：

环球律师事务所数据合规团队专注于网络安全与数据合规、个人信息隐私保护等领域。我们在企业境内外数据合规体系建设等方面具备丰富的经验，为多家大型互联网公司、全球企业提供法律与咨询服务。

我们为客户提供在网络安全与数据合规、个人信息隐私保护、跨境数据传输、电子商务与广告合规领域的法律咨询及相关方案设计，帮助客户迎接数据时代的机遇与挑战。

孟洁
合伙人律师
直线：86-10-6584-6768
总机：86-10-6584-6688
邮箱：
mengjie@glo.com.cn

一、新规速递

1. 美国 CCPA 1 月 1 日生效，企业需要注意哪些事项

2020 年 1 月 1 日，美国加州 CCPA 正式施行。CCPA 全称是 2018 年加州消费者隐私法案，这部法律出台的目的是当科技公司收集和使用数据时，赋予人们更多的信息和数据控制权。

CCPA 的颁布标志着加州成为美国第一个具有完整用户隐私法律的州。它虽然仅适用于加州公民，但鉴于这部法律的全面性和高覆盖率，其每项条款都对从事个人数据收集和处理的企业有着巨大影响。

如果说欧盟 GDPR 为保护公民隐私开了一个好头，那么加州 CCPA 则继往开来。众所周知，欧盟 GDPR（即《通用数据保护条例》）于 2018 年 5 月 25 日正式生效。这部“大法”不仅取代了 1995 年的《数据保护指令》和欧盟成员国各自制定的相关法规，而且在个人隐私保护方面迈出一大步。

一旦违反 GDPR，后果很严重。例如，2019 年 7 月 8 日，英国信息监管局发表声明说，英国航空公司因违反 GDPR 被罚 1.8339 亿英镑（约合 15.8 亿元人民币）。

欧盟 GDPR 从步伐上开创了隐私保护的新时代，而加州 CCPA 或许将从影响力上推动隐私保护再前进一步。

硅谷科技公司的态度

鉴于加州的独特地位，我们或许可以看到 CCPA 的潜在影响。

加州经济发达。根据 2018 年美国商务部的数据显示，加州 GDP 高达 2.747 万亿美元。如果把它视为独立经济体，加州经济规模能排到全球第五，对全美、乃至全球经济影响巨大。更重要的是，加州是硅谷所在地，汇集着谷歌、Facebook、惠普、英特尔、苹果、思科、英伟达、甲骨文和特斯拉等科技大公司和众多创业公司。目前，有些公司已经采取相关措施，促使平台合规：

Twitter：

2019 年 12 月，Twitter 公司宣布一项新的“隐私中心”，更新其隐私政策。

谷歌：

针对 CCPA，谷歌则推出一款 Chrome 插件，它可以允许人们禁用 Google Analytics 收集其信息。

Mozilla：

“自我要求”更高的 Mozilla 在 2020 年 1 月 1 日宣布，它计划新的一年里在全球范围遵守 CCPA，而不仅仅针对美国加州公民。并且，Mozilla 在声明中指出，它收集的用户数据非常少。在即将到来的更新中，Mozilla 计划让用户能从 Mozilla 的服务器上删除他们的遥测数据。

Facebook:

Facebook 称，无需更改政策，因为它表示从技术上讲，自己不会“出售”用户数据，而是将其用于广告定位。

根据加州发布的一份报告表明，预计科技公司将花费约 550 亿美元来实现合规性。

虽然不菲的合规成本会暂时影响某些科技公司的发展，但如果能早日实现合规，那么这些科技公司或许会“活得更久”。

加州 CCPA VS 欧盟 GDPR

尽管加州 CCPA 吸取了欧盟 GDPR 的一些理念，比如数据访问权、数据删除权和数据可携带权，但是很多方面比欧盟相关条例更具体。

当然，欧盟的条例中有些内容则是加州法案所没有的。我们可以看看两者的相同和差异。

对比项	CCPA	GDPR	分析
1.哪些企业受到监管？	满足以下条件之一的加州企业，属于本法律的适用范围： 年收入超过 2500 万美元；拥有超过 50000 个消费者、家庭或设备的商业数据；消费者个人数据的销售额占年收入一半以上。本法律也适用于以下企业：上述企业的控股公司或者被控股公司；与上述企业共享品牌的公司，例如，共享企业名称、服务商标或注册商标。 本法律部分条款还适用于：服务供应商和第三方。	对于数据控制者和数据处理者而言：不管数据处理发生地是否在欧盟范围内，只要是欧盟国家企业，在欧盟机构活动的背景下处理个人数据；即使是非欧盟国家企业，只要其处理的欧盟数据主体个人数据，与欧盟范围内的产品或服务相关，或与行为监测相关；都必须遵守本条例。	欧盟 GDPR 的应用范围和地域范围要大得多。受到监管的企业范围也有较大不同。
2.哪些人受到保护？	本法律所保护的加州居民须满足以下任一条件： 在加州境内且非短暂停留的人；定居在加州但暂时不在加州境内的人；本法律所保护的消费者群体包括： 居家用品和居家服务的消费者；公司员工；企业对企业的交易（B2B 交易）	数据主体，具体指与个人数据相关的已识别或可识别的个人。	两部法律在定义方式上差异大，但影响同样广泛；虽然两部法律聚焦的数据都与可识别的自然人有关，但对数据的定义不同；两部法律对地域之外的对象都有潜在影响，管辖范围之外的企业也受影响。
3.哪些信息受保护？	特定消费者或家庭的个人信息，信息类型主要包括可识别、可描述、能产生联系、或直接间接产生关联的信息；法律定义包括一系列特	与已识别或可识别数据主体相关的所有个人数据；除非有合法理由，否则欧盟 GDPR 禁止处理任何特殊类型的个人	两部法律在信息的定义上基本相似，唯一不同的是加州 CCPA 还覆盖家庭和设备层

	定种类的个人信息；个人信息不包括公开的政府记录。另外本法律同样不包括其他法规所覆盖的个人信息。	数据。	面的信息。
4.隐私声明或知情权的规定	企业必须告知消费者以下内容： 企业采集的个人信息种类；每个种类拟定的使用目的；如果企业有以下操作，还需进一步告知： 企业要采集附加的个人信息种类；采集个人信息用于其他不相关的目的；CCPA 要求企业向消费者提供特定信息，建立交付需求；第三方在从其他企业获取数据时，也必须给予消费者明确的通知，让消费者在转售个人信息之前有机会选择退出。	数据控制者必须对其个人数据采集和处理提供细节信息。不论信息采集是直接来自数据主体还是来自第三方，都必须让消费者知情。	两部法律在信息披露规定方面比较类似，只是特定信息的获取方式和交付方式有所不同；CCPA 规定：如果消费者提出请求，企业必须向消费者出示个人信息披露或转卖给第三方的相关信息，但内容只涵盖到消费者提出请求前的 12 个月。
5.数据安全	CCPA 没有强制规定数据安全的条款，但针对企业不顾现存加州法律风险，违反数据安全操作规则所引发的数据泄露，本法律规定了诉讼权。	GDPR 要求数据控制者和数据处理者采取合理的方式和组织措施，确保与风险相匹配的安全水平。	在司法方式上基本相同，但随着组织环境和监管机构的理解不同，合理的安全措施一定程度上也不尽相同。
6.关于儿童的权利规定	CCPA 规定，企业未经允许，禁止出售 16 周岁以下消费者的个人信息；年龄 13-16 周岁的儿童可以直接给予企业同意。13 周岁以下的儿童须经父母同意。需要	GDPR 默认年满 16 周岁的儿童才有决定自己个人信息如何处理的权利，但欧盟成员国法律的年龄规定是 13-16 周岁。13 周岁以下的儿	除了年龄区间的规定相似之外，两部法律的区别很大。CCPA 只在个人数据出售方面需要父母同意，而 GDPR 规定所有数据

	明确的是，本法律遵从《联邦儿童在线隐私保护法》提供的保护条款。	童须由其监护人提供同意的权利；儿童必须要收到一份与其年龄相适应的隐私说明；儿童的个人数据必须受到更高层级的安全要求监管。	处理过程都必须经过父母同意。
7.关于信息的删除权或被遗忘权	除个别例外情况，消费者有权删除企业采集的个人数据；企业也必须通知其服务供应商删除相应数据。	在六种情况下，数据主体有权删除个人数据；数据控制者必须采取合理措施，告知同样处理数据的其他数据控制者。	两部法律在数据删除权方面的规定类似；欧盟 GDPR 关于数据删除权实施的情况只规定了六种情况，而 CCPA 更宽泛；欧盟 GDPR 规定企业有义务通知下游数据接受者删除个人数据，这一点的适用范围也比较宽泛。
8.反歧视规定	企业处理消费者数据时，不能歧视消费者；除非消费者提供的数据价值有差异，否则企业的定价不能因歧视而厚此薄彼；如果财务激励措施在条款中或线上隐私政策有呈现，而且需要消费者的一致应允，企业才能为消费者提供财务激励。	类似的反歧视规则在 GDPR 中体现得比较含蓄。关于相关组织不能在数据主体行使其权利时予以歧视，例如禁止对数据主体权利和自由造成影响的数据处理行为，条例没有明确说明。	两部法律在该方面所体现的观念相同，但对义务的规定不同。
9.惩罚措施（私人诉权）	对数据泄露包括信息的部分泄露，CCPA 的惩罚措施没那么宽泛。如果发生数据泄露，企业有 30 天时间修复；消费者每人单次事件可以寻求实际赔偿金或法律赔	GDPR 可对数据控制者或数据处理者造成物质或非物质的损失进行处罚。	两部法律的适用范围差异比较大，但违规行为都会产生重大经济责任。

	偿金，金额从 100 美元到 750 美元不等。法院也可以指令或公告形式对企业进行减免。		
10.惩罚措施（民事罚款）	加州总检察长对于每次违规行为判决的民事罚款约 2500 美金，如果是故意行为，最高可达 7500 美金。但本法律规定，企业有 30 天的时间修复数据泄露问题。	行政处罚最高可达 2000 万欧元，或该企业全年收入的 4%；根据欧盟 GDPR 第八十三条，欧盟成员国实施罚金处罚应遵照 GDPR 违反章程，而非各国的行政处罚。	虽然罚金的计算方式不同，但是欧盟 GDPR 的处罚显然更重。

回看中国，在个人隐私方面，主要有两种糟糕的现象：一是侵犯用户隐私，比如一些 App 违规收集、使用用户个人信息、不合理索取用户权限等；二是买卖个人数据。

几年前，个人数据或信息买卖非常猖獗，很多都是明码标价，比如手机号多少钱一个、身份证号多少钱一个、银行卡号多少钱一个，这些全部明码标价。

欧盟 GDPR 之后，出现加州 CCPA，而 CCPA 后，将有中国的相关法律出台。据悉，在隐私保护方面，中国正在制定《个人信息保护法》和《数据安全法》，预计 2020 年出台。

从欧盟、美国到中国，个人隐私保护已经成为互联网时代的重要命题。这个命题的前提是，数据被视为新时代的“石油”，它有着无限价值。经济利益的驱使，加上技术的滥用，个人数据被疯狂掠夺，这一切让个人隐私保护进入“黑暗时期”。而 GDPR、CCPA 和中国正在制定的法律或许能成为冲破黑暗的一束光。[1]

[1] InfoQ。

2. 信安标委发布《个人信息告知同意指南》《移动互联网应用（App）收集个人信息基本规范》等标准的征求意见稿

2020 年 1 月 20 日，全国信息安全标准化技术委员会在官网上发布了包括《信息安全技术 个人信息告知同意指南》等标准的征求意见稿，面向社会广泛征求意见，截止时间为 2020 年 3 月 20 日。[2]

征求意见的标准以及对应的链接如下：

《信息安全技术 个人信息告知同意指南（征求意见稿）》

https://www.tc260.org.cn/file/2020-01-21/9f800dc2-b2e0-40c1-9847-0a5a690b8e5b.docx

《信息安全技术 移动互联网应用（App）收集个人信息基本规范（征求意见稿）》

https://www.tc260.org.cn/file/2020-01-20/cb2dd4d9-b6ee-4cdf-bcb6-fdf46a04b5b7.docx

《信息安全技术 云计算服务安全指南（征求意见稿）》

https://www.tc260.org.cn/file/2020-01-20/e31b37b2-4e59-4586-839f-9a940b7fffca.doc

《信息安全技术 云计算服务安全能力要求（征求意见稿）》

https://www.tc260.org.cn/file/2020-01-20/d11e4a6e-ae54-4d9b-8be8-989b3605c44a.docx

[2] 全国信息安全标准化技术委员会。

《信息安全技术 车载网络设备信息安全技术要求（征求意见稿）》

https://www.tc260.org.cn/file/2020-01-20/4b6a24e6-7373-408e-81f2-293b9f02834f.docx

《信息安全技术 智能门锁安全技术要求和测试评价方法》

https://www.tc260.org.cn/file/2020-01-17/35d63993-45e4-48f8-8948-42fc2169e701.doc

《信息安全技术 网络入侵检测系统技术要求和测试评价方法（征求意见稿）》

https://www.tc260.org.cn/file/2020-01-20/e16acc33-457f-4de5-9e65-7196f230ec15.doc

《信息安全技术 网站数据恢复产品技术要求与测试评价方法（征求意见稿）》

https://www.tc260.org.cn/file/2020-01-20/9e3dc860-0480-46f6-8dfd-6b30c4009f79.docx

《信息安全技术 数据备份与恢复产品技术要求与测试评价方法（征求意见稿）》

https://www.tc260.org.cn/file/2020-01-20/fe86d096-dedd-43bf-9d49-eccb9f61b07a.docx

《信息安全技术 网络脆弱性扫描产品安全技术要求和测试评价方法（征求意见稿）》

https://www.tc260.org.cn/file/2020-01-20/45288ae2-16ba-4cf0-8f97-456b834f9ce3.doc

《信息安全技术 信息安全服务分类（征求意见稿）》

https://www.tc260.org.cn/file/2020-01-16/ca54caee-061a-4b21-84ab-15ba2c0db2b4.docx

《信息安全技术 信息安全风险管理指南（征求意见稿）》

https://www.tc260.org.cn/file/2020-01-17/4491a940-2d46-4f5d-9225-5d819267e23b.docx

《信息安全技术 网络身份服务安全技术要求（征求意见稿）》

https://www.tc260.org.cn/file/2020-01-20/396117b5-4ece-4d2e-83ab-a84360d909ce.doc

《信息安全技术 互联网信息服务安全通用要求》

https://www.tc260.org.cn/file/2020-01-20/2d3fdbbc-28ad-4095-9ec6-b3c56c239c3b.doc

《信息安全技术 公钥基础设施 标准符合性测评》

https://www.tc260.org.cn/file/2020-01-20/6c66ad71-84f5-47b7-8126-228727cd7bc4.doc

二、监管动态

1．央行拟在 1 月 20 日左右上线第二代个人征信系统

央行征信中心第二代个人征信系统暂定于 1 月 20 日上线，具体确定时间以后续公告为准。对个人来说，二代征信系统所展示的个人信用信息将更加具体，但由于升级前后向征信系统报送数据的机构和数据种类没有大的变化，因此，对个人经济生活的影响不会发生太大变化。

要点一：对个人经济生活影响不大

2006 年，全国集中统一的企业和个人征信系统正式上线，信用报告已成为反映企业和个人信用行为的“经济身份证”。截至 2019 年 4 月底，个人和企业征信系统已采集 9.9 亿自然人、2591.8 万户企业和其他组织的信息，分别接入机构 3564 家和 3465 家，年度查询量分别达到 17.6 亿次和 1.1 亿次。

从纳入数据情况看，央行征信中心副主任王晓蕾近日表示，截至 2019 年 11 月底，个人征信系统接入各类放贷机构共 3693 家，已经基本实现对个人金融信用信息的广覆盖。当前，我国征信系统依法合规采集的反映借款人信用状况的信息，主要包括三类：

一是个人信贷信息，包括贷款、信用卡、担保等业务信息。

二是“先消费后付款”的信用信息，主要包括电信等公用事业缴费信息，这类信息可以帮助缺少信贷记录的个人建立信用档案。

值得注意的是，新版信用报告设计了水、电、电信等公用事业缴费信息的展示格式。央行征信中心自 2006 年开始探索采集反映个人信用状况的“先消费后付款”的公用事业缴费信息，并最先从采集个人电信正常缴费和欠费信息开始探索，其中欠费信息只采集欠费 2 个月以上的信息。但根据《征信业管理条例》第十三条“采集个人信息应当经信息主体本人同意，未经本人同意不得采集”规定，在采集公用事业缴费信息的实际操作中，必须先征得信息主体本人同意，未经本人同意不得采集，也就不会在个人征信报告中呈现这部分信息。

王晓蕾曾表示，信用报告采集公用服务缴费信息时会遵循两方面原则：一是公

用信息采集之前必须征得本人同意，采集负面信息必须告知个人；二是如果本人对信息持有异议，可以提出异议，央行会与数据源单位协商，如果确有误会立即纠正。

三是公共信息，主要包括行政许可与处罚信息、法院失信被执行人信息等。

总体看，征信系统运行十多年，信用报告的基本结构和内容已基本稳定。新版信用报告的改进，主要在优化界面展示、提升可读性方面做了调整。仅就本次升级而言，由于升级前后向征信系统报送数据的机构和数据种类没有大的变化，因此，对个人经济生活的影响不会发生太大变化。

不过，即将上线的新版信用报告与目前的信用报告版本相比，还是增加了一些信息，如：个人基本信息中增加了国籍等信息，信贷信息中增加了共同借款、个人为法人担保、法人为个人担保等信息。

此外，在还款记录的展示方面，新版记录也有更新完善。新版个人信用报告设计展示“5 年还款记录”（包括还款状态、逾期金额），现行个人信用报告也展示了 5 年的还款记录，只是展示方式略有差异，具体体现在延长了个人正常还款信息的记录时间。

现有的信用报告中，对于个人不良借贷记录等负面信息的保存期限是 5 年，即对自不良行为或者事件终止之日起为 5 年，超过 5 年期限后从信用报告中删除；对于个人正常还款记录等正面信息的保存期限则是 2 年。相比之下，新版信用报告中，对于上述负面和正面还款信息的保存期限统一调整为 5 年，也就是延长了个人正常还款记录的保存期限，其目的在于更好地展示信息主体的信用状况，帮助公众积累信用财富，促进获得融资。

要点二：婚姻状况内容来自个人向金融机构提供的信息

近日，有市场传闻称，新版信用报告上线后，因新增了“共同借款”信息，离婚后即便是非主贷人，买房时也无法再享受首套房贷认定资格。实际上，这一说法并不完全准确。

究竟何为共同借款？央行有关负责人此前表示，所谓“共同借款”是指一笔贷款由两个或两个以上借款人共同承担连带偿还责任的借款。根据国际征信实践，共同借款信息会同时展示在每个借款人的信用报告中，金融机构在评估借款人信用风险时会把共同借款信息考虑在内。征信中心积极探索在新版信用报告中增加“共同

借款”信息采集内容，本着“尊重事实”原则，将借款信息同时展示在每个借款人信用报告中，如实反映借款人负债情况。如后续借款主体发生变更，征信系统将按照金融机构的上报信息，及时更新信息，客观记录实际情况。

现有的个人信用报告中虽没有直接显示“共同借款”信息，但金融机构可以间接查询到。如信用报告中会显示婚姻状况，金融机构可以结合借款人的本人信用状况及其婚姻状况中显示的配偶相关信息，来自行判断共同借款情况。相比之下，新版信用报告只是将共同借款情况以更直接的方式明确展示出来而已。

值得注意的是，即便新版信用报告中增加“共同借款”信息采集内容，但信息采集的前提是基于“尊重事实”的原则。而何为“事实”，就是金融机构与借款人签订的借款合同。如果合同上借款人是 A 的名字，则这笔借贷信息会反映在 A 的信用报告中；如果合同借款人是 A 和 B 的名字，则这笔借贷信息不仅会反映在 A 的信用报告中，也会反映在 B 的信用报告中。

同时，婚姻状况变更后对共同借款的影响，更多需要个人主动到借贷银行更新信息，银行会将最新信息反馈给征信系统，这样可以确保信用报告中信息的准确性和有效性。新版信用信息更新也将更及时，各机构需要在采集时点 T+1 向征信中心报送数据，以前可能需要一个月甚至更久才能更新征信数据。

要点三：个人有权对不良信息作出说明并记载

个人征信报告每年有两次免费查询的机会，公众可以通过人民银行征信中心官方网站、全国各地人民银行分支机构设立的查询点，及部分金融机构网点、部分地区政务大厅进行柜台或自助查询机查询。王晓蕾建议公众一年查询两次，一方面，能发现本人信用信息是否存在问题；另一方面，在发现错误信息后能够及时纠正。

一旦个人对自己信用报告上的信息有异议，可以向征信中心或银行提出异议申请更正。征信中心应自收到异议之日起 20 日内进行核查和处理，并将结果书面答复异议人。

值得注意的是，个人有一项权利不应忽视。按照《征信业管理条例》第十六条规定，“在不良信息保存期限内，信息主体可以对不良信息作出说明，征信机构应当予以记载。”也就是说，个人拥有在信用报告中对不良信息进行说明的权利，以便金融机构查询时作为参考。

此外，尽管个人可以对自己的信用报告自由查询，但每次查询都会记录在报告中，一些金融机构会将信用报告的查询次数作为贷款、信用卡等申请时的信用风险分析依据。个人若在申请贷款前短期内过于频繁查询，金融机构可能会谨慎放贷。因此，个人也要注意控制查询次数。[3]

2. 工信部通报下架第一批侵害用户权益 App 名单

2019 年 12 月 19 日，工信部部向社会通报了 41 家存在侵害用户权益行为 APP 企业的名单。截至 1 月 3 日，经第三方检测机构核查复检，尚有 3 款 APP 未按要求完成整改。依据《网络安全法》和《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407 号）等法律和规范性文件要求，工信部对上述 APP 进行下架。[4]

下架的 3 款 App 名单参见以下链接：

https://mp.weixin.qq.com/s/UUrG-G3fjNCaFOelrXJiMA

3. 工信部通报下架第二批侵害用户权益 App 名单

1 月 8 日，工信部通报第二批侵害用户权益行为 APP。通报显示，存在问题的应用软件共 15 款。

通报中介绍，根据《工业和信息化部关于开展 APP 侵害用户权益专项整治工作的通知》要求，工信部按计划、分阶段、稳步推进 APP 侵害用户权益专项整治行动，专项行动期间，第一批未按要求完成整改的 3 家企业，已于 1 月 3 日依法组织下架。现将第二批发现存在问题且未完成整改的 15 款 APP 向社会通报。该 15 款 App 存在的问题包括：

1. 私自收集个人信息；

[3] 证券时报。
[4] 工信微报。

2. 私自共享给第三方；

3. 不给权限不让用；

4. 过度索取权限；

5. 账号注销难；

6. 强制用户使用定向推送功能等问题。

工信部要求，被通报的 APP 应在 2020 年 1 月 17 日前完成整改落实工作。逾期不整改的，工信部将依法依规组织开展相关处置工作。[5]

此次下架的 15 款 App 名单以及问题参见以下链接：

https://mp.weixin.qq.com/s/wSsWO9e-3glzsRH7tnCqVg

4. 国家计算机病毒应急处理中心发现 24 款违法 App

1 月 13 日，国家计算机病毒应急处理中心近期在“净网 2020”专项行动中通过互联网监测发现，多款违法、违规有害移动应用存在隐私不合规行为，违反《网络安全法》相关规定，涉嫌超范围采集个人隐私信息。

违法、违规移动应用存在的问题具体如下：

1、未经用户同意收集个人隐私信息，涉嫌隐私不合规。

2、未向用户明示申请的全部隐私权限，涉嫌隐私不合规。

针对上述情况，国家计算机病毒应急处理中心提醒广大手机用户首先不要下载这些违法有害移动应用，避免手机操作系统受到不必要的安全威胁。其次，建议

[5] 工信微报。

打开手机中防病毒移动应用的“实时监控”功能，对手机操作进行主动防御，这样可以第一时间监控未知病毒的入侵活动。[6]

被通报的 App 清单参见以下链接：

http://www.xinhuanet.com/2020-01/13/c_1125455263.htm

5. 教育部： 1 月 31 日前必须完成所有教育 App 备案，目前已有 628 个教育 App 完成备案

针对不久前，央视新闻曝光河南、云南、江苏等地出现的一些电信运营企业利用“校讯通”等由头进入校园，变相要求学生和家长下载指定的 App，并开展增值收费业务的情况，教育部科技司司长雷朝滋在接受央视新闻独家专访时表示，进入校园的 App 是不允许应用垄断的，也不允许强制收费，也不允许擅自采集个人信息，教育部对这此类乱象将会加强监管。

随着网络技术发展和资本的涌入，教育类 App 发展飞速，但也出现了一些问题。近两年，央视新闻持续对中小学生培训类的 App 乱象进行了曝光，教育部相关负责人表示，此次对全国范围内的教育 App 进行集中统一备案，就是要加强对违法违规行为的监管。

据央视记者梳理，**自 2018 年起，教育部已经相继出台《教育部办公厅关于严禁有害 App 进入中小学校园的通知》、《教育部等六部门关于规范校外线上培训的实施意见》、《教育部等八部门关于引导规范教育移动互联网应用有序健康发展的意见》和《教育移动互联网应用程序备案管理办法》**，政策频出的背后，正是着力规范这一新兴领域。

2019 年 12 月 19 日，工信部通报了第一批侵害用户权益行为的 App，41 款 App 被要求整改，其中包括学霸君 1 对 1、智学网、互动作业帮 3 款教育类 App。教育部科技司司长雷朝滋表示，已和工信部、中央网信办进行沟通，对涉事的教育 App 的整改进行跟踪。未来，教育部也将建立教育 App 的常态化监管机制，在教育 App 的动态监管上进行制度建设。除了地方教育行政部门和相关部门加强监管，企业自身加强自我约束以外，教育部还将设置相关的举报渠道，对企业的发展，对

[6] 新华社。

教育 App 的健康发展进行促进。

日前，教育部公布了新一批教育 App 备案名单，1 月 31 日前将完成对全国范围内所有教育 App 的备案工作。作为首次对全国范围内教育 App 开展集中统一备案工作，备案工作自去年 12 月开展，已有 303 家企业的 628 个教育 App 通过了备案审核。

教育部科技司司长雷朝滋表示，开展备案工作，就要加强对全国教育 App 的事中、事后监管。这一次实施的教育 App 备案是对所有学段的，不止针对某一个学段，覆盖各级各类教育。教育 App 是以教职工、学生和家长为主要用户，以教育教学学习作为主要应用场景，涉及到教师教学、学生学习、家长互动等方方面面。这些都属于此次要备案的 App 的范畴。

据了解，教育 App 备案的过程为，提供者在今年 1 月 31 日前完成 ICP 备案和等级保护备案，并在教育移动互联网应用程序备案系统上传信息，以完成备案。此次备案工作，教育 App 的提供者实行“一省备案，全国有效”的原则，即教育 App 在注册地备案后，在其他地区开展业务无须重复备案。教育部相关负责人表示，“属地备案”也将应用于教育 App 备案后的监管当中。

针对监管问题，教育部科技司司长雷朝滋表示，因为 App 可能在所在地的省用，可能会覆盖到别的省。别的人反馈问题，我们还是会反馈到企业所在地的教育行政部门，让它们进行监管。当然，中央有关部门也可以对教育 App 使用的情况进行相应的监管。[7]

6. 全国政协召开网络议政远程协商会 围绕“加强大数据时代个人信息保护”协商议政

全国政协 1 月 10 日在京召开网络议政远程协商会，议题是“加强大数据时代个人信息保护”。中共中央政治局常委、全国政协主席汪洋主持会议并讲话。他强调，要深入学习贯彻习近平总书记关于网络安全和个人信息保护工作的重要指示精神，以发展的眼光和辩证的思维看待大数据时代个人信息保护问题，坚持以人民为中心，坚持政府监管、行业自律、社会参与统筹推进，坚持标本兼治，在提高信

[7] 央视新闻。

息资源利用水平的同时科学有效保护信息安全，让大数据更好服务社会、造福人民。

14 位委员与专家在全国政协机关和辽宁、安徽、湖南、贵州 5 个会场以及通过手机连线方式发言，近 120 位委员通过移动履职平台发表意见。大家认为，党中央高度重视大数据时代个人信息保护，有关方面做了大量工作，取得了积极成效。但传统个人信息保护制度和方式跟不上互联网广泛普及和数字产业迅猛发展的新形势，相关法律法规不完善、多头监管与监管缺失并存、企业主体责任落实不到位、公民自我保护意识不强等问题较为突出，维护信息安全依然任重道远。

一些委员建议，要加快出台专门的个人信息保护法律，明确个人信息概念、适用对象和权属，明确采集、处理、使用个人信息的程序、规则和相关责任。要加大专项治理力度，重拳打击非法收集、交易、使用个人信息的违法犯罪活动，提高违法违规成本，最大限度挤压网络黑灰产业生存空间。要实施分级分类保护，建立个人信息利用清单，强**化对人脸识别、数据爬取等技术应用和“人肉搜索”等行为的监管。**要压实企业主体责任，**引导企业建立健全内部管控机制**，克服重发展轻安全的倾向。要广泛宣传个人信息安全知识、技术和理念，增强公民自我保护意识，不给违法犯罪行为以可乘之机。要加强部门间信息共享和统筹协调，建立统一的个人信息保护监管平台，避免多头执法和重复执法。

全国政协副主席张庆黎、夏宝龙、辜胜阻、邵鸿出席会议。政协委员张英、陈晓红、景亚萍、赖明勇、朱山、吴杰庄、王小川、童国华、王悦群、汪利民、谈剑锋、方来英、崔仑和专家杜跃进作了发言。中央网信办、工业和信息化部、公安部、卫生健康委、市场监管总局等部门负责同志现场作了互动交流。[8]

7. 人民网、中国信息通信研究院、中国互联网协会共同发布《移动互联网应用用户个人信息保护十大倡议》

人民网、中国信息通信研究院、中国互联网协会共同发起了《移动互联网应用用户个人信息保护十大倡议》

1 月 10 日，由公安部网络安全保卫局指导、人民网和中国信息通信研究院联合主办、巨掌互动科技协办的首届移动互联网应用安全发展峰会在人民日报社新

[8] 央广网。

媒体大厦举行。

本届峰会以“5G 互联安全先行”为主题，邀请相关部委领导、专家学者、知名 APP 企业代表、媒体代表等 300 余人齐聚一堂，围绕“5G 时代移动互联网的安全隐患和风险防范”等议题，共同探讨如何打造更安全、更可靠的移动应用市场，助力行业健康有序发展。

为加强行业自律，强化产业协作体系，为用户提供更安全放心的移动互联网应用服务，人民网联合中国信息通信研究院、中国互联网协会共同发起了《移动互联网应用用户个人信息保护十大倡议》。来自中国普天、浪潮、百度、顺丰速运、首汽约车、字节跳动、平安集团、高德地图等 60 余家企业代表参与倡议，共同维护行业健康有序发展。[9]

“十大倡议”全文如下：

(一)加强行业自律，明确企业主体责任

严格遵守法律法规，全面加强行业自律。行业自律是用户个人信息保护的关键，也是企业可持续发展的内在基础。鼓励企业在行业协会的组织下，严格遵守法律法规，积极开展自律工作。应用服务和应用分发厂商积极落实主体责任，主动适应个人信息保护和数据管理新形势新要求，严格遵守法律法规，贯彻落实个人信息收集使用规定，不断完善企业内部的个人信息保护和数据管理制度，持续优化用户隐私政策，并将个人信息保护的要求贯彻执行到规划、开发、运营等各个环节，积极配合主管部门的监管要求，切实有效维护好用户合法权益。

(二)依托公众监督，及时响应用户关切

高度重视用户权益保障，为用户举报监督创造便利条件。公众监督是保障用户权益的重要渠道，也是约束企业行为的有效方式。应用服务、应用分发平台应以用户为中心，为用户举报投诉设置便捷的方式和渠道，健全公众参与监督的机制，时刻关注用户感受和体验，尊重并保障用户的投诉权和可追溯权，积极向行业主管部门移交公众举报信息。

[9] 同花顺财经。

(三)规范收集使用规则，落实告知同意

规范告知明示内容，确保用户知情权、选择权。收集使用规则是用户了解移动互联网应用用户个人信息收集使用的主要渠道，收集使用规则应满足清晰、明确、完整、易懂等要求，确保用户充分理解。收集使用规则应包含收集使用信息的内容、目的、方式、范围、频次、保护措施以及公开、转移、共享等相关信息。移动应用服务商应严格依照收集使用规则进行用户个人信息收集处理，遵循告知同意原则，在收集用户个人信息前，以易于感知的方式，明示告知用户收集使用规则，待用户同意后，方可执行。

(四)规范信息共享规则，明确责任归属

根据信息共享和责任归属原则，增加信息可追溯性。移动应用服务商应制定清晰、明确的信息共享规则，在转移、共享用户个人信息前，应先明示用户共享的内容、共享对象、共享用途等相关信息，征得用户同意后，方可转移或共享信息。移动应用服务商应与信息接收方订立安全协议，明确各方信息保护责任，并要求信息接收方依规执行。

(五)规范推送及权限调用，加强用户可知可控

加强应用推送及权限调用管理，净化应用环境。完善的应用推送及权限调用管理机制可以有效约束应用服务在未向用户告知或未以显著方式标示情况下，将收集到的用户搜索、浏览记录、使用习惯等个人信息用于定向推送或精准营销的行为。构建应用服务合规合理定向推送，净化移动互联网应用环境，以期提高公众对应用服务的使用信心。

(六)提高应用防护能力，保障用户合法权益

提高安全专业能力，高度重视个人信息保护。安全防护能力是移动应用保护用户个人信息的基础保障。移动应用开发者应采取必要的手段保障应用的安全性和用户数据的机密性、完整性和可用性。应用服务开发者应将安全编码原则贯穿整个软件开发周期，采用高等级 API 和安全 SDK、适配最新操作系统及外部代码库、尽量减少代码的攻击面。并对应用进行必要的安全加固、采用安全存储和传输技术保障用户敏感信息安全，通过完善的身份认证机制保障通信过程安全。

(七)规范平台信息声明，保证下载用户知情

为用户提供应用详情，增加应用环境透明度。应用平台信息声明是用户了解应用基本信息的重要途径。平台应明示用户，应用名称、功能描述、卸载方法、开发者信息、应用安装及运行所需权限列表等，明确告知用户应用收集使用用户个人信息的内容、目的、方式和范围等。在用户下载应用时，平台应明示应用名称、功能描述、卸载方法、开发者信息、应用安装及运行所需权限列表等，且应明示用户收集使用个人信息的内容、目的、方式和范围。

(八)完善安全审核职责，落实分发上架机制

通过应用检查审核机制，为用户提供合规应用。应用分发平台审核机制是保证用户个人信息的基础保障。平台应审核开发者资质和应用相关信息。平台应制定明确的上架要求并建立完备的检测机制，通过自动化检测和人工审核手段，对应用收集使用用户个人信息的行为进行规范。应用分发平台应对应用进行跟踪监测和管控，包括定期复查，定期对已上架的应用进行复查，发现问题立即下架。

(九)健全投诉反馈渠道，配合监管落实规范

根据反馈保障机制，为用户提供可查可控途径。应用分发平台承担连接用户、应用及终端的桥梁责任，是用户个人信息保护工作的重要环节。应用分发平台应建立多种途径及时接收和反映用户的建议和投诉，并通过既定规则流程，及时响应用户投诉和应用侵权审核情况。平台应积极支撑主管部门开展市场监测工作，敦促落实用户信息收集使用规则，辅助主管部门进行监管和决策。

(十)加强多方沟通协调，强化产业协作体系

针对焦点和难点问题，产业界齐心协力联手行动。针对焦点和难点问题，产业界齐心协力联手行动。针对当前用户普遍关注的移动互联网应用用户个人信息安全问题，产业界应积极响应产业诉求，加强终端厂商、应用服务商、应用分发商、安全厂商等多方面的沟通协调，在设备安全、应用安全、数据安全等多方面加强交流合作，共享技术经验，制定行业标准规范，强化产业协作体系，共同提升移动互联网应用用户个人信息保护能力。

三、相关案例

1. 电信运营商内鬼倒卖个人信息已受法院审判

近日，中国裁判文书网公布了《陈德武、陈亚华、姜福乾等侵犯公民个人信息罪二审刑事裁定书》。经法院二审审理查明：2013 年至 2016 年 9 月 27 日，被告人陈亚华利用职务之便，从号百信息服务有限公司（为中国电信股份有限公司的全资子公司）数据库获取区分不同行业、地区的手机号码信息提供给陈德武，被告人陈德武以人民币 0.01 元/条至 0.2 元/条不等的价格在网络上出售，获利金额累计达人民币 2000 余万元，涉及公民个人信息 2 亿余条。

号百信息服务有限公司是中国电信股份有限公司的全资子公司，公司于 2007 年 8 月 16 日在上海挂牌成立，注册资本 3.5 亿人民币。

公诉机关指控：2013 年至 2016 年 9 月 27 日，被告人陈亚华从号百信息服务有限公司（以下简称“号百公司”）数据库获取区分不同行业、地区的手机号码信息提供给陈德武，被告人陈德武以人民币 0.01 元/条至 0.2 元/条不等的价格在网络上出售，获利金额累计人民币 2000 余万元，涉及公民个人信息 2 亿余条。被告人王玉自 2015 年开始受被告人陈亚华指使帮助陈亚华从“号百公司”数据库获取公民个人信息发送到指定邮箱。被告人陈德武将被告人陈亚华提供的公民个人信息出售获得的赃款部分分给陈亚华。

被告人姜福乾于 2014 年 1 月 3 日至 2016 年 9 月 27 日，以人民币 0.08 元/条至 0.12 元/条不等的价格向被告人陈德武购买公民个人信息 1235 万余条，支付人民币 1482418 元，以人民币 0.09 元/条至 0.1 元/条不等的价格在网络上出售给王某 6、赵某 2、张某 3、高某、张某 4 等人。

被告人杨奚于 2014 年 2 月 14 日至 2016 年 9 月 25 日，以人民币 0.1 元/条至 0.2 元/条不等的价格向被告人陈德武购买公民个人信息 299 万余条，支付人民币 448630 元，将购得公民个人信息的 80%左右以购买原价出售给其所在公司的下属员工张某 1、刘某 3、徐某、盛某等人，被告人杨奚及其下属员工利用购得的公民个人信息进行经营活动，获利金额达人民币 5 万元以上。[10]

[10] 财经网。

2. 航空公司员工泄露明星信息受到处分

近期，国航员工在个人社交媒体上泄露大量明星个人信息，甚至乘机记录。事件发生后，引发了社会舆论及高度关注。国航官方紧急发布了声明，称确有员工严重违反数据管理相关规定，目前已经对该员工作出停飞处分，同时也向此事涉及的旅客表示最真诚的道歉。此事件的发生反应出以下多个问题，这些问题值得我们深思。

1、人们对个人信息保护重视程度不断提高

随着大数据的发展，个人隐私保护愈发受到人们的重视，捍卫个人数据安全，不被偷窥和打扰成为迫切的需求。同时，随着国家相应的政策的出台，也给重要行业及涉密机构提出了更高的要求。

2、重要信息被轻易截取，无任何技术性防控措施

抛开职业操守与素养，航空部门是否应该增加自身防范能力，面对信息泄露等类似情况有能力阻止或者快速追溯泄露原因。

3、访问权限过低

据了解，该员工为普通乘务人员，一名普通员工就能获得如此重要的乘客信息，说明航空公司设置了过低的访问权限，或者甚至可能没有访问权限，任何内部人员随意调取。

内部泄露已成为数据泄露事件的主要通道，据《2019 年内部数据泄露调查》显示，61%的公司数据存在被员工恶意泄露的风险。nCipher Security 公司发布的 2019 年全球加密趋势研究显示，员工失误被列为企业数据泄露的最高风险，90%外部网络攻击的发生是因为员工无意中向黑客提供了其访问权限。

涉密企业或数据价值较高的企业应引起足够重视。事实上，利用职务之便泄露他人隐私的案件并非孤例。近年来，从航班内鬼泄露明星出行信息， 到江苏镇江一医院工作人员疯狂追星，公然倒卖印有明星隐私的医药包，再到物流快递行业，出现大面积泄露姓名、联系方式等个人隐私的情况，这其中有的出于经济利益，有的是单纯为了满足虚荣心，还有的是工作大意疏忽导致。

调查发现，企业绝大多数安全措施都侧重于阻止外部的恶意窥探数据的行为，却忽视了内部员工在无意或恶意的情况下造成的内部数据泄露的风险。

重点企业及涉密机构应与专业的数据安全机构合作利用有效的技术手段，兼顾商业运行的同时，加强对敏感信息访问权限的管控，在储存及传输的数据时进行加密处理，同时当面对无法预测的泄露时有对数据追溯的能力。商务密邮作为邮件安全提供商，从邮件数据加密到邮件数据管控，满足不同行业用户对邮件安全的需求，全面防控数据不泄露。[11]

3. 缴获公民个人信息 98 亿条，广东警方“净网 2019”专项行动战果丰硕

2019 年广东公安强力组织开展“净网 2019”专项行动，严厉打击网络突出违法犯罪，强力整治网络违法有害信息，全面整改网络安全风险隐患，努力推动构建网络综合治理体系，全年共侦破网络主侦案件 2960 余起，刑事拘留 10420 余人，同比分别上升 29.03%、25.16%；缴获公民个人信息 98 亿条，发现整改网络高危隐患 6350 余个，监测拦截网络攻击 2461 万次，网络空间综合治理能力大幅提升。

据了解，“净网 2019”专项行动围绕网络犯罪的推广、技术、帐号、支付等关键环节，严厉打击侵犯公民个人信息、黑客攻击破坏两大上游性源头性犯罪，以及其他黑灰产业链条上的犯罪，深入开展网络违法犯罪生态治理，全年共侦破网络主侦案件 2963 起，刑事拘留 10421 人，同比上升 29.03%、25.16%，缴获公民个人信息 98 亿余条；推动构建“单位自防、行业联防、社会协防、公安打防”的网络安全罩综合防控体系，将关键信息基础设施纳入安全罩进行整体防护，目前已经纳入防护的重点行业信息系统和党政机关网站 10350 个，全年共发现整改网络高危隐患 6352 个，监测拦截网络攻击 2461 万次，封堵 IP60 万多个，及时发现处置网络安全事件 2116 起；全网域整顿网络公共秩序，依托省市县三级网上巡查责任体系和 24 小时巡查处置机制，及时清理整治涉黄赌毒、涉枪爆、涉网络诈骗等违法有害信息，并逐条倒查涉及到的网站和 IDC 等，全年共处置网上违法有害信息 6.79 万余条，累计倒查纳管网站 3.34 万个、IDC1140 家。

广东省公安厅网警总队相关负责人表示，接下来，广东警方将继续组织开展“净网 2020”专项行动，强化网络空间综合治理，不断提升维护网络安全的能力和

[11] 信息安全调查员 008。

水平，全力营造清朗的网络空间。

典型案例：“净网 15 号”打击利用网贷 APP 非法获取公民个人信息专案

2019 年上半年，广州警方在对某“套路贷”犯罪团伙侦查过程中发现，该团伙运营一款具有非法采集公民个人信息功能的“套路贷”APP，该款 APP 由西安某天游金融信息服务有限公司开发。该公司同时为全国 300 多家公司开发各式各样的网贷 APP，每款收益为 8 万元至 25 万元，此类 APP 在未明确告知用户的情况下，非法采集注册用户的身份信息（身份证、户籍等）、手机信息（通话记录、通讯录等）、网购信息（购物记录、收货地址）、支付信息（余额、交易记录）等隐私数据，受害人涉及全国 28 个省市、135 万余人、13 多亿条公民信息。

此外，该利用其 APP 非法采集的公民信息数据，以及从杭州魔某数据科技有限公司、上海某颜征信服务有限公司等购买的公民信息数据开发“某创 AI 网贷平台”，对借款人进行大数据风控分析，得出贷款人的借贷风控报告提供给网贷公司作放贷业务参考，以此非法获利。

在查清团伙组织架构和锁定相关犯罪证据后，在公安部和省公安厅的统一指挥下，广州警方对西安信天游金融信息服务有限公司和下游的“套路贷”团伙展开收网，抓获犯罪嫌疑人 94 人，缴获公民个人信息 13 亿条，打掉下游“套路贷”犯罪团伙 9 个。该案是生态打击“套路贷”犯罪产业链条的典型案件。

警方在此表示，公安机关将对“套路贷”犯罪涉及的技术服务商、数据服务商、支付服务商、推广服务商开展生态式、全链条打击，互联网从业公司和人员要增强法律意识，千万不要成为套路贷”犯罪的“帮凶”。[12]

4. 银行 APP 被点名后陆续更新隐私条款 预防数据泄露需“双管齐下”

2019 年 12 月份，国家网络安全通报中心通报有 100 款违法违规采集个人信息的 APP 被查处，其中多款金融类 APP 赫然在列。当月 30 日，国家网信办、工信部、公安部、国家市场监管总局联合发布《APP 违法违规收集使用个人信息行为认定方法》(以下简称《认定方法》)，明确了六大违规行为。

[12] 南方新闻网。

《认定方法》发布后，在上述 100 款被点名的 APP 中，一些金融类 APP 陆续更新隐私条约，收敛信息采集范围或开始新增用户服务提示，在收集和使用用户信息方面更加规范。

一位银行业人士表示，监管部门和金融机构应该联合制定一套严格规范的流程和制度，专门针对 APP 软件的安全问题进行管控，包括从软件的开发、使用到维护等全部生命周期的覆盖，确保系统平稳运行。同时，对泄露个人信息的人员应进行严厉处罚，对相应的金融科技公司也要有更加完善的考核机制。

被点名金融类 APP 已陆续更新隐私条款

近年来，随着互联网和新技术的不断发展，科技已深入生活的方方面面。但是在带给人们便捷的同时，也潜在很多风险。在大数据时代，个人信息的安全尤为重要。

《认定方法》发布后，部分银行类 APP 迅速予以回应。例如，在《认定方法》发布的第二天，被点名的某银行 APP 发布的最新手机银行用户隐私政策已经非常详实，对银行将如何收集个人信息，收集信息的范围有哪些，将如何使用用户个人信息，如何使用 Cookie 和同类技术，如何共享、转让、公开披露个人信息，如何保护、存储个人信息等与银行收集与使用个人信息的方方面面进行了非常细致的描述。并对在办理业务时，每一类业务将要涉及到收集的信息内容以加粗字体的形式着重显示。与此前的隐私政策相比，在手机用户信息的收集范围上明显缩减。

另一个被点名的某地方性银行，近期进行了多次“更新”。在苹果 App Store 中，该行曾在 1 个月前被点名时发布新版本，更新客户隐私协议内容；在 3 周前，新增 APP 隐私政策授权提示；今年 1 月 2 日，也就是《认定方法》发布的 3 天后，更新版本新增用户服务协议提示。此外，该行的 APP 用户隐私政策也对如何收集及使用，转让和公开披露，存储和保护、管理个人信息以及保护未成年人信息等进行了详细描述。

总体来看，此次被“点名”的银行都在 APP 上更新或发布了手机银行用户隐私政策。同时，还有多个在线贷款类 APP，也在被点名后更新了用户隐私政策。但相对于银行因各种业务会涉及需求不同的信息，在线贷款类 APP 隐私政策的更新相对更简单。

金融类 APP 成信息泄露重灾区

在各类 APP 过度收集使用用户信息的通报中，包括银行在内的金融类 APP 都是常客，其中不乏大型银行和互联网金融行业的头部公司。

金融类 APP 不同于其他 APP，此类 APP 涉及到个人信息的采集通常更为全面和严格，因此金融类 APP 也是信息泄露的重灾区。现在很多金融服务都可以在线上完成，带来了极大的方便。在线上办理业务会要求个人录入信息，甚至包括面部识别和指纹。一旦这些信息被泄露，拿去做不法的事情，后果不敢想象。

中国信息通信研究院日前发布的《2019 金融行业移动 APP 安全观测报告》显示，截至 2019 年 9 月 11 日，该报告团队从 232 个安卓应用市场中收录了 133327 款金融行业 APP，其中，面向个人用户的消费金融类 APP 数量最多，占观测总数的 36.74%。根据上述报告，发现有 70.22%的金融行业 APP 存在高危漏洞，攻击者可利用这些漏洞窃取用户数据、进行 APP 仿冒、植入恶意程序、攻击服务等，对 APP 安全具有严重威胁。其中排名前三的高危漏洞均存在导致 APP 数据泄露的风险。

区块链技术可解决个人信息被盗问题

要防止银行信息不被泄露，还需要技术与监管双管齐下。既然有信息的买方，就会有不法分子为此盗取信息。无论是技术上的保障，还是从业人员的监管，都必须配套更完善的措施。

央行科技司司长李伟在 2019 年 12 月份表示，2019 年底对金融类 APP 开展标准测评和认证后，注意到几部委开展的对 APP 风险的整治，其中银行类 APP 是风险重灾区，所以将加快推进有关工作，切实防范化解风险。李伟同时宣布成立国家金融科技测评中心，致力于开展金融科技应用测评、风险监测以及监管科技与合规科技建设。

李伟称，目前央行正积极推动现金、机具等方面强制性国家标准出台，抓紧研究涉及人工智能、区块链、大数据、云计算等领域 17 项行业标准。他特别提到，今年 9 月央行发布的《移动金融客户端应用软件安全管理规范》，就是一个推荐性的标准，从风险防控、信息保护、实名备案、监督处置等方面，提出了针对性的要求。

区块链技术可以很好地解决个人信息被盗问题，因为这是区块链的主要功能之一，也就是确定权属关系。比如，信息所有权是谁？这个信息是带有时间戳的，不能随意篡改，每次使用都有记录。

通过给数据和信息确权，不仅可以防范个人信息泄露这样的安全事件，也使信息数据变成了个人财产。当这些数据被用于经济活动，比如交易、消费者画像等，会产生价值，这个价值在区块链确权后就归属于明确的产权人，不能被商家随意占有。即使目前还未有相关的应用平台出现，但相信未来会被不断发展和应用。信息确权对数字经济时代来说，是一个革命性的功能。[13]

5. 转卖个人信息 50 余万条，37 名嫌犯被抓

近日，新乡县公安局组织刑侦、网监、经侦、交警等多警种联动，成功破获一起新乡市多家装修公司涉案的侵犯公民个人信息案件，抓获犯罪嫌疑人 37 名，捣毁贩卖公民信息窝点 6 处，扣押涉案电脑 43 台、手机 100 余部、移动硬盘、U 盘 41 个，查获涉及豫北地区公民数据 50 余万条，案件涉及省内鹤壁、平顶山、安阳、新乡等多个地区。

恼人电话全是推销装修

2019 年 8 月 5 日，新乡县公安局网络监察大队民警接到某公司员工王某的举报电话，称其经常无故接到新乡市多家公司的推销电话，每次都是在向推销房屋装修，这让王某非常苦恼。民警意识到，很可能是王某的个人信息被盗取。民警深入调查后发现，该公司多名人员的身份信息被盗取买卖。公民信息属于个人的隐私，个人信息泄露很可能影响群众的正常生活，甚至对公民的人身安全造成危害。新乡县公安局党委书记、局长张忠文要求主管刑侦的副局长张吉林立即抽调精干民警成立专案组，全力侦办此类案件。网络监察大队大队长郭春雨，教导员王学忠，刑警大队二中队李永杰、岳素武、申佳伟、时鹏飞针等民警立即对前期调查的线索逐条核查、深挖跟进。

循线深挖贩卖信息网络浮出水面

经过近两个月的侦查，北京某装饰公司新乡市加盟公司的杜某(男，43 岁，新乡县人)、马某(男，33 岁，新乡市红旗区人)被民警纳入视线。专案民警立即行动，将涉案的杜某、马某抓获。民警在其公司电脑中发现了上传云端的大量个人信息。经审讯，马某如实交代了自 2019 年以来伙同杜某加盟北京某装饰公司，通过网络非法购买公民在售楼部、房屋中介、医院、银行、小区物业的个人信息，然后高价卖给和公司有业务往来的新乡市多家装修公司。据马某交待，有时卖出高档小区业

[13] 证券日报。

主的一条个人信息就能获利上百元。装修公司购买个人信息后，根据业务需要进行电话推销装修业务。

民警顺线追踪、连续作战，又发现新乡市某广告公司的吕某(男，36 岁，辉县市人)、李某(男，43 岁，辉县市人)、师某(男，35 岁，辉县市人)等人为获取利益非法买卖个人信息。根据查获的线索，民警扩展调查，一张遍布新乡市区非法购买个人信息的 20 余家装修公司浮出水面。鉴于案情重大、涉及人员多，新乡县公安局决定，前期锁定证据，伺机集中抓捕。

协调联动摧毁贩卖公民信息窝点

在获得新乡市公安局的支持后，副局长张吉林带领专案组精干力量研判分析、精准落地，梳理出涉嫌该案的上线、下线犯罪嫌疑人，制定了详细的抓捕方案。新乡市犯罪侦查支队、新乡县公安局刑警大队、网监大队、经侦大队、交警大队 100 余名民警开展统一收网行动，先后抓获犯罪嫌疑人 37 名，查获获取的个人信息 50 余万条，成功破获该起侵犯公民个人信息案件。

目前，涉案的 35 人被公安机关采取刑事强制措施，两人被行政处罚。案件正在进一步侦办中。[14]

6. 通过监听通讯公司与互联网公司信息、监控手机移动设备识别码等，美国“棱镜计划”精准定位伊朗指挥官苏莱曼尼

2020 年 1 月 3 日，美军空袭杀死了伊朗伊斯兰革命卫队特种部队“圣城旅”指挥官卡西姆·苏莱曼尼。

在国际上曝光“棱镜计划”的前美国中情局技术分析员斯诺登指出，1 月 3 号苏莱曼尼被精确追踪，完全是美国“棱镜计划”的功劳。原理是，通过监听通讯公司与互联网公司信息和监控苏莱曼尼的诺基亚手机移动设备识别码等，从而定位到其具体位置，完成对其击杀。

据悉，为了避免暴露自己，苏莱曼尼使用的是一款老式的诺基亚手机，里面没

[14] 大河网。

有植入任何 APP，并且还经过高级加密，不可能被跟踪以及窃听。即便如此，美军依然做到了对其的精准打击。

美军此举引发一系列连锁反应，随后的 1 月 8 日，美军驻伊拉克“阿萨德空军基地”遭到“数十枚导弹”袭击。据伊朗法尔斯通讯社报道这仅是此次苏莱曼尼被杀后伊朗反击行动的第一步。

中东事件引起国际广泛关注，有人问：特朗普是否也会被追踪？

前不久，《纽约时报》旗下的一个专栏 Time Opinion 近日曾发布的一个关于隐私的重磅调查引发全民热议，其中显示了通过手机记录的数据，研究人员成功还原了总统特朗普一天的行踪。

根据 Time Opinion 发布的总统特朗普行踪轨迹，可以清晰看到：从早晨 7 点 10 分起，特朗普的手机亮点在佛罗里达州棕榈滩海湖庄园里出现，9 点 24 分，手机亮点出现在特朗普在当地的高尔夫俱乐部，特朗普在此地和日本首相安倍晋三打高尔夫球，一直呆到下午 1 点 12 分。中午特朗普回来和其他人一起享用了一顿私人午餐。下午 5 点 08 分，手机亮点又回到海湖庄园，当晚，特朗普又和安倍共进工作晚餐。甚至，他们还可以追踪白宫、五角大楼、联邦调查局、国会大厦、最高法院等几乎每个政府大楼中的智能手机，从而确定被追踪者的真实身份。

报道称，这些数据并不是来自电信公司或大型科技公司，也不是来自政府情报部门。它最初来自一个位置数据公司，在每个人的手机上，可能都有十几个 App 在悄悄收集这些信息。

国际社会牵一发而动全身的复杂局势并非一人能够左右，但此次美国将信息技术应用于军事行动的着实让人震惊。面对可怕的“精准定位”，也许，对于任何有数据访问权的人来说，我们的生活就是完全公开的。

试想，我们使用的手机都是经过实名登记和注册的，国际巨头的政客都能通过手机被发现，对于我们普通个人数据隐私，包括姓名、收入、性别、年龄、职业、健康和经济状况等，甚至我们所在的位置，在面对任何有数据访问权的人时，这一切被一览无遗并非不可能。[15]

[15] SCA 联盟。

7. 受加州新隐私法推动 Firefox 将允许用户删除其收集的数据

据外媒 CNET 报道，Firefox 浏览器制造商 Mozilla 表示，它使所有用户都可以更好地控制自己的数据。这项改变是由《加州消费者隐私法案》(CCPA)推动的，该法案于周三正式生效。新的数据隐私法赋予加州居民了解科技公司收集哪些个人数据的权利。它还使人们可以要求公司删除其数据，而不是将其出售。Mozilla 表示，根据 CCPA 进行的更改将适用于每个 Firefox 用户，而不仅限于加州的用户。

Mozilla 在周二发布的一篇博文中表示，它将使 Firefox 用户可以选择删除该公司在下一版浏览器（该版本将于 1 月 7 日发布）中收集的数据。Firefox 不会在浏览网站或进行搜索查询时收集数据。Mozilla 表示，它将允许用户选择删除遥测数据，其中包括打开了多少标签或会话持续了多长时间。Mozilla 称，它使用这些数据来改善 Firefox 的性能和安全性。

包括微软在内的其他公司也表示，将把新法律要求的权利扩展到加州以外的用户。该公司表示，法律的要求符合其认为隐私是一项基本人权的信念。

出于意识形态或实践原因，可能会有更多公司效仿。一些法律观察家表示，一些公司可能认为为两个州的用户创建两个不同的界面，或者确定哪些用户符合法律规定的加州居民资格是不值得的。此外，其他州也考虑了类似的隐私法，因此未来的要求可能会超出加州。

CCPA 还禁止公司歧视依法行使权利的用户，并允许用户起诉公司因疏忽造成的数据泄露。CCPA 与欧洲的《通用数据保护条例》相似，该条例于 2018 年生效。[16]

8. 亚马逊员工泄露客户数据 回应：已解雇涉事人员

1 月 12 日上午消息，亚马逊一周以来第二次承认其员工不正确地访问了客户数据。

亚马逊周五通知客户，在发现几名员工与第三方共享客户电子邮件地址和电

[16] cnBeta。

话号码后，他们解雇了这几名员工。

亚马逊发言人在一份声明中说："对此事件负责的个人已经被解雇，我们正在支持执法部门对他们的起诉。"

亚马逊表示，没有其他用户信息被共享。但该公司拒绝透露有多少名员工被解雇，以及受此事件影响的客户数量或为何与第三方共享信息。

亚马逊在发给客户的电子邮件中表示，员工与第三方共享数据的行为违反公司政策。

在本周的另一起事件中，亚马逊宣布解雇了四名 Ring 员工，原因是他们滥用对客户视频源的访问权限。亚马逊表示，Ring 现在将"此类数据访问限制在少数团队成员内"，并将继续审查对这些特权的访问，以确定"他们是否需要继续访问客户信息"。

亚马逊在 2018 年 10 月承认了另外一起几乎相同的事件，该公司当时因为与第三方共享客户电子邮件地址而解雇了一名员工。在 2018 年 11 月，亚马逊也披露了一起事件，其中有数目不详的用户名和电子邮件地址因为"技术错误"而遭到泄露。

第三方卖家对于亚马逊的整体业务已变得越来越重要，这使其可以大大扩展其网站上可用产品的选择。现在，该市场占亚马逊总销售额的一半以上，吸引了数百万在该平台上销售产品的第三方卖家。[17]

9. 某知名跨国公司 Access 数据库呈现缝隙，或导致敏感信息泄露

外媒报道称，有研究人员发现微软的 Access 数据库应用程序存在漏洞，如果不及时进行修补，可能会导致敏感信息的意外泄露，或将导致 8.5 万家企业面临风险。不过截止目前，还并未有公司声明受到了损害。

Microsoft Access 在很多地方都得到广泛使用，尤其是小型企业，以及大公司的相关部门，能够极大地提高工作效率。原因就在于 Access 一可以用来进行数据

[17] 新浪科技。

分析，它拥有超强的数据处理、统计分析能力，利用其查询功能，用户可以轻松地进行各类汇总、平均等统计。并可灵活设置统计的条件。比如在统计分析上万条记录、十几万条记录及以上的数据时速度快且操作方便，这一点是 Excel 无法与之相比的。

据悉，此次所发现的漏洞与去年在 Microsoft Office 中发现的漏洞非常相似。不过，Access 是随机地将称为内存元素的数据片段保存到每个文件中。通常情况下，这些内容都是无效内容，但是偶尔里面也会包含有一些敏感信息，比如比如密码或用户信息之类的内容。这些数据对于普通人而言毫无价值，但是对于一个有耐心的黑客而言，这些信息极具价值。

Mimecast 表示，被黑客入侵之后，黑客可以在这些内容中开启自动检索功能，然后从中获取敏感信息，这些信息可以被用于任何恶意用途。目前，Microsoft 已发布补丁来更正此问题，Mimecast 鼓励企业下载并安装该补丁，并实时监控网络流量，以监视是否有攻击者在搜索潜在敏感文件的情况。[18]

[18] 大话科技堂。

四、环球评论

1. 《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范（征求意见稿）》10.24 与 1.20 版对比

2020 年 1 月 20 日，信安标委在其官网张公布了《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范（征求意见稿）》，与 2019 年 10 月 24 日发布的版本相比，标准正文部分存在以下变动：[19]

10.24 版	1.20 版
1　范围	1　范围
本标准明确了移动互联网应用程序收集个人信息时应满足的基本要求，用以规范移动互联网应用程序运营者收集个人信息的行为。	本标准明确了移动互联网应用程序收集个人信息时应满足的基本要求，用以规范移动互联网应用程序运营者收集个人信息的行为。
本标准适用于移动互联网应用程序的开发和运营，也可用于移动互联网应用程序的技术评估、监督检查。	本标准适用于移动互联网应用程序的开发和运营，也可用于移动互联网应用程序的技术评估、监督检查。
2　规范性引用文件	2　规范性引用文件
下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。	下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。
GB/T 25069—2010　信息安全技术　术语	GB/T 25069—2010　信息安全技术　术语
GB/T 35273　信息安全技术　个人信息安全规范	GB/T 35273　信息安全技术　个人信息安全规范
3　术语与定义	3　术语与定义
GB/T 25069—2010、GB/T 35273中界定的以及下列术语和定义适用于本文件。	GB/T 25069—2010、GB/T 35273中界定的以及下列术语和定义适用于本文件。

[19] 作者：孟洁律师团队。

3.1 智能移动终端 intelligent mobile terminal 安装有开放式操作系统，能使用无线移动通信技术实现互联网接入，通过下载、安装应用软件和数字内容为用户提供服务的终端产品。 3.2 移动互联网应用程序 mobile internet application 安装、运行在智能移动终端上的应用程序，简称App。 3.3 服务类型 service type 移动互联网应用程序所提供的满足个人信息主体具体使用需求的业务功能。 3.4 最小必要信息 minimum necessary personal information 保障某一服务类型正常运行所最少够用的个人信息，包括一旦缺少将导致该类型服务无法实现或无法正常运行的个人信息，以及法律法规要求必须收集的个人信息。 3.5 最小必要权限范围 minimum necessary permission range 用于收集某一服务类型最小必要信息且需要个人信息主体主动授予的智能移动终端操作系统权限。	3.1 智能移动终端 intelligent mobile terminal 安装有开放式操作系统，能使用无线移动通信技术实现互联网接入，通过下载、安装应用软件和数字内容为用户提供服务的终端产品。 3.2 移动互联网应用程序 mobile internet application 安装、运行在智能移动终端上的应用程序，简称App。 3.3 服务类型 service type 移动互联网应用程序所提供的满足个人信息主体具体使用需求的业务功能。 3.4 最小必要信息 minimum necessary personal information 保障某一服务类型正常运行所最少够用的个人信息，包括一旦缺少将导致该类型服务无法实现或无法正常运行的个人信息，以及法律法规要求必须收集的个人信息。 3.5 最小必要权限范围 minimum necessary permission range 用于收集某一服务类型最小必要信息且需要个人信息主体主动授予的智能移动终端操作系统权限。
3.6 移动互联网应用程序运营者 mobile internet application operator 移动互联网应用程序的所有者、管理者和移动互联网应用程序服务的提供者。	3.6 移动互联网应用程序运营者 mobile internet application operator 移动互联网应用程序的所有者、管理者和移动互联网应用程序服务的提供者，简称App运营者。
4 App 收集个人信息基本要求 App收集个人信息应满足以下要求：	4 App 收集个人信息基本要求 App收集个人信息应满足以下要求： a)App 运营者应履行个人信息安全保护义务，

a) App 运营者应履行个人信息安全保护义务，采取必要措施，保障个人信息安全;	采取必要措施，保障个人信息安全；
/	b)App 应以制定隐私政策等方式公开收集使用个人信息规则；
b) App 应在首次运行时通过弹窗等明显方式向个人信息主体告知收集最小必要信息规则，如隐私政策的核心内容;	c)App 应在首次运行时通过弹窗等明显方式向个人信息主体告知收集最小必要信息规则，如隐私政策的核心内容；
c) App 运营者不应在征得个人信息主体授权同意前，产生个人信息收集行为;	d)App 运营者不应在征得个人信息主体授权同意前，产生个人信息收集行为；
/	e)App 运营者不应在个人信息主体明确表示不同意后，仍通过技术等其他手段继续收集个人信息；
d) 当个人信息主体同意 App 收集某服务类型的最小必要信息时，App 运营者不得因个人信息主体拒绝提供最小必要信息之外的个人信息而拒绝提供该类型服务; 注:附录 A 列举了 App 常见的服务类型以及服务类型对应的最小必要信息。	f)当个人信息主体同意 App 收集某服务类型的最小必要信息时，App 运营者不应因个人信息主体拒绝提供最小必要信息之外的个人信息而拒绝提供该类型服务； 注：附录 A 列举了 App 常见的服务类型以及服务类型对应的最小必要信息。
e) 除法律法规的强制性要求，App 运营者不得收集与所提供的服务无关的个人信息;	g)除法律法规的强制性要求外，App 运营者不应收集与所提供的服务无关的个人信息；
f) App 运营者不得收集不可变更的设备唯一标识(如 IMEI 号、MAC 地址等)，用于保障网络安全或运营安全的除外;	h)App 运营者不应收集不可变更的设备唯一标识（如 IMEI 号、MAC 地址等），用于保障网络安全或运营安全的除外；
g) 个人信息主体明确拒绝使用某服务类型后，App 运营者不得频繁(如每 48 小时超过一次)征求个人信息主体同意使用该类型服务，并保证其他服务的正常使用; 注:个人信息主体主动触发导致的征求同意相关提示除外。	i) 个人信息主体明确拒绝使用某服务类型后，App 运营者不应频繁（如每 48h 超过一次）征求个人信息主体同意使用该类型服务，并保证其他服务的正常使用； 注：个人信息主体主动触发导致的征求同意相关提示除外。
h) 在 App 运营者使用第三方代码或插件满	j)在 App 运营者使用第三方代码或插件满足

足其特定功能时，如该第三方代码或插件具备个人信息收集功能且个人信息主体无法拒绝的，App 运营者应确保第三方代码或插件履行个人信息安全保护义务，并防止第三方代码或插件收集无关的个人信息; 注:如第三方代码或插件自行向个人信息主体明示其收集、使用个人信息的目的、方式、范围， 并征得个人信息主体的授权同意，则第三方代码或插件独立对其个人信息收集行为承担责任。	其特定功能时，如该第三方代码或插件具备个人信息收集功能且个人信息主体无法拒绝的，App 运营者应确保第三方代码或插件履行个人信息安全保护义务，并防止第三方代码或插件收集无关的个人信息； 注：如第三方代码或插件自行向个人信息主体明示其收集、使用个人信息的目的、方式、范围，并征得个人信息主体的授权同意，则第三方代码或插件独立对其个人信息收集行为承担责任。
i) 当 App 运营者拟收集的个人信息超出服务类型的最小必要信息时，对于超出部分的个人信息，App 运营者应征得个人信息主体的授权同意。涉及个人敏感信息的， 应逐项征得个人信息主体的明示同意;	k)当 App 运营者拟收集的个人信息超出服务类型的最小必要信息时，对于超出部分的个人信息，App 运营者应征得个人信息主体的授权同意。涉及个人敏感信息的，应逐项征得个人信息主体的明示同意；
j) 当~~同一~~App 有两种或两种以上服务类型时，App 运营者应允许个人信息主体逐项开启和退出服务类型，开启或退出的方式应易于操作;	l)当 App 有两种或两种以上服务类型时，App 运营者应允许个人信息主体逐项开启或关闭服务类型，开启或关闭的方式应易于操作；
k) 除法律法规的强制性要求外，当个人信息主体关闭某服务类型后，App 运营者应终止该服务类型收集个人信息的活动，并对仅用于该服务的个人信息进行删除或匿名化处理; 注:关闭服务类型包括个人信息主体明确表明放弃使用该服务类型、或通过操作关闭该服务类型相关的交互式界面等。	m)除法律法规的强制性要求外，当个人信息主体关闭某服务类型后，App 运营者应终止该服务类型收集个人信息的活动，并对仅用于该服务的个人信息进行删除或匿名化处理； 注：关闭服务类型包括个人信息主体明确表明放弃使用该服务类型、或通过操作关闭该服务类型相关的交互式界面等。
l) 当 App 申请个人信息相关权限或要求个人信息主体输入个人信息时，App 运营者应向个人信息主体同步明示申请权限或收集信息的目的;	n)当 App 申请个人信息相关权限或要求个人信息主体输入个人信息时，App 运营者应向个人信息主体同步明示申请权限或收集信息的目的；
m) App 运营者应向个人信息主体提供实时查询已从该个人信息主体所收集个人信息类型的途径;查询结果应通过在 App 开设独立	o)App 运营者应向个人信息主体提供实时查询已从该个人信息主体所收集个人信息类型的途径；查询结果应通过在 App 开设独立界

界面的方式展示，且查询方式应易于操作。	面的方式展示，且查询方式应易于操作；
~~n) 存在共享、转让个人信息的，App 运营者应向个人信息主体提供实时查询数据接收方身份的途径;查询结果应通过在 App 开设独立界面的方式展示，且查询方式应易于操作。~~	/
/	p)通过间接方式收集个人信息的，App 运营者应向个人信息主体提供实时查询数据提供方身份的途径；查询结果应通过在 App 开设独立界面的方式展示，且查询方式应易于操作；
o) 在技术可行且不影响终端和服务正常的情况下，App 运营者应优先在个人信息主体的智能终端中存储、使用所收集的个人信息。	q)在技术可行且不影响终端和服务正常的情况下，App 运营者应优先在个人信息主体的智能移动终端中存储、使用所收集的个人信息；
p) App 运营者应以实现服务所必需的最低合理频率向其后台服务器发送个人信息。	r)App 运营者应以实现服务所必需的最低合理频率向其后台服务器发送个人信息。

在附录部分，所列举的常见服务类型由原来的 21 种变为 30 种，增加了旅游服务、酒店服务、网络游戏、在线影音、儿童教育、电子图书、拍摄美化、应用商店、网络直播场景下的最小必要信息。以下标黄部分为 0120 版新增内容，红色加删除线为此次删去的部分。

A.1 地图导航

为用户提供互联网地图和导航功能。该服务类型的最小必要信息如表 1 所示：

表 1 地图导航类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。

实现服务所需个人信息	位置信息 • 精准定位信息 • 行踪轨迹	精准定位信息仅用于确定用户位置，提供地图搜索展示和导航服务。 行踪轨迹仅用于在导航服务中判断实时路况及重新规划导航路线。

A.2 网络约车

为用户提供网络预约汽车（不包含汽车租赁）服务。该服务类型的最小必要信息如表 2 所示：

表 2 网络约车类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	手机号码	《移动互联网应用程序信息服务管理规定》
	用户发布的信息内容 身份认证信息 订单日志 上网日志 行驶轨迹日志	《网络预约出租汽车经营服务管理暂行办法》
	交易信息	《电子商务法》 《网络交易管理办法》 《网络预约出租汽车经营服务管理暂行办法》
实现服务所需个人信息	账号信息 • 账号 • 口令	仅用于标识网络约车用户和保障账号信息安全。
	位置信息 • 精准定位信息 • 用户出发地 • 用户到达地	精准定位信息仅用于确定用户当前位置，推荐周围上车点，搜索显示附近车辆信息。

类型	个人信息	使用要求/相关法律法规依据
	第三方支付信息	仅用于用户使用第三方支付方式对约车订单付款，通常包括支付时间、支付金额、支付渠道等。
	仅在客服场景下收集： 客服沟通记录和内容 • 通话录音（电话客服） • 聊天消息（在线客服）	仅用于客服处理用户纠纷，具体包括电话客服和在线客服。

表 2 所列个人信息为网络约车乘客的个人信息，不包含网络约车驾驶员的个人信息。

此外，为保证行程安全，保障司乘合法权益，网络约车服务过程中还可能记录行程录音信息。

A.3 即时通讯

为用户提供在线文字、语音、视频等形式的通讯服务，或基于即时通讯的交友互动等服务。该服务类型的最小必要信息如表 3 所示：

表 3 即时通讯类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	手机号码	《网络安全法》 《移动互联网应用程序信息服务管理规定》 《互联网群组信息服务管理规定》

类型	个人信息	使用要求/相关法律法规依据
	仅对使用信息发布功能的用户收集： 用户日志信息 • 账号、操作时间、操作类型、网络源地址和目标地址、网络源端口、客户端硬件特征 • 通讯群组名称、昵称、简介、备注、标识 • 用户信息发布、转发、评论记录	《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》
	仅对公众账号信息发布服务使用者收集： 身份认证信息 • 姓名 • 证件类型 • 证件号码	《互联网用户公众账号信息服务管理规定》
实现服务所需个人信息	账号信息 • 账号 • 口令 • 昵称 • 头像	仅用于标识即时通讯用户、保障账号信息安全和用户聊天交流。
	好友列表	仅用于建立和管理用户在即时通讯应用的联系人关系。 应允许用户在即时通讯应用中手动添加好友，而不应强制读取用户的通讯录。
	好友信息 • 好友账号 • 好友昵称 • 好友头像	仅用于向用户展示好友基本信息，或经本人同意后授权第三方平台登录使用。
	群列表	仅用于实现群组聊天功能。

A.4 ~~博客论坛~~网络社区

为用户提供博客、论坛、社区等服务，包括话题讨论、信息分享和关注互动等功能。该服务类型的最小必要信息如表 4 所示：

表 4 网络社区类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	手机号码	《网络安全法》 《移动互联网应用程序信息服务管理规定》 《互联网群组信息服务管理规定》
	仅对使用信息发布功能的用户收集： 用户日志信息 • 账号、操作时间、操作类型、网络源地址和目标地址、网络源端口、客户端硬件特征 • 通讯群组名称、昵称、简介、备注、标识 • 用户信息发布、转发、评论记录	《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》
	仅对公众账号信息发布服务使用者收集： 身份认证信息 • 姓名 • 证件类型 • 证件号码	《互联网用户公众账号信息服务管理规定》
实现服务所需个人信息	账号信息 • 账号 • 口令 • 昵称 • 头像	仅用于标识网络社区用户、保障账号信息安全和用户互动交流。

类型	个人信息	使用要求/相关法律法规依据
	用户关注记录 • 关注的内容 • 关注用户列表	关注的内容仅用于建立和管理用户和社区内容（如关注的栏目、关注的话题等）的关注关系，以及向用户展示和推送关注的内容。 关注用户列表仅用于建立和管理网络社区用户间的关注关系，以及向用户展示和推送关注的用户发布的图文资讯、音视频、链接等。 应允许用户在网络社区应用中手动设置关注用户，而不应强制读取用户的通讯录。
	仅在客服场景下收集： 客服沟通记录和内容 • 通话录音（电话客服） • 聊天消息（在线客服）	仅用于客服处理用户纠纷，具体包括电话客服和在线客服。

A.5 网络支付

为用户提供在收付款人之间转移货币资金的服务（如非银支付、网银支付），包括支付、提现、转账、账单等功能。该服务类型的最小必要信息如表 5 所示：

表 5 网络支付类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	手机号码	《移动互联网应用程序信息服务管理规定》
	身份基本信息 • 国籍 • 性别 • 职业 • 住址 • 联系方式	《支付机构反洗钱和反恐怖融资管理办法》

类型	个人信息	使用要求/相关法律法规依据
	身份证件信息 • 姓名 • 身份证件种类 • 身份证件号码 • 身份证件有效期限 • 身份证件复印件或影印件	《非金融机构支付服务管理办法》
	国际移动设备识别码（IMEI）	《非银行支付机构反洗钱现场检查数据接口规范（试行）》
	客户操作行为	《非银行支付机构网络支付业务管理办法》
	交易信息	《电子商务法》 《网络交易管理办法》
实现服务所需个人信息	账号信息 • 账号 • 口令	仅用于标识网络支付用户和保障账号信息安全。
	银行账户信息 • 开户行名称 • 银行卡号码 • 银行卡有效期限 • 银行预留手机号码	仅用于实现银行卡和支付账号绑卡、银行卡身份认证、充值、提现、转账功能。
	交易身份验证信息（用户支付时可任选一种） • 静态密码 • 数字证书 • 电子签名 • 动态密码	仅用于对用户真实身份进行验证，以确保用户账户与资金安全。
	仅在客服场景下收集： 客服沟通记录和内容 • 通话录音（电话客服） • 聊天消息（在线客服）	仅用于客服处理用户纠纷，具体包括电话客服和在线客服。

A.6 新闻资讯

为用户提供图文、音视频等新闻资讯信息服务，包括新闻资讯的浏览、搜索和发布功能。该服务类型的最小必要信息如表 6 所示：

表 6 新闻资讯类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	仅对使用信息发布功能的用户收集： 手机号码	《网络安全法》 《移动互联网应用程序信息服务管理规定》 ~~《互联网群组信息服务管理规定》~~
	仅对使用信息发布功能的用户收集： 用户日志信息 • 账号、操作时间、操作类型、网络源地址和目标地址、网络源端口、客户端硬件特征 • 通讯群组名称、昵称、简介、备注、标识 • 用户信息发布、转发、评论记录	《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》
	仅对公众账号信息发布服务使用者收集： 身份认证信息 • 姓名 • 证件类型 • 证件号码	《互联网用户公众账号信息服务管理规定》
实现服务所需个人信息	关注的账号	仅用于向用户展示和推送关注的账号所发布的新闻资讯。

A.7 网上购物

为用户提供网上购买商品或服务的服务类型，包括商品展示、搜索、下单、交付、客服售后等功能。该服务类型的最小必要信息如表 7 所示：

表 7 网上购物类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	手机号码	《网络安全法》 《移动互联网应用程序信息服务管理规定》
	交易信息	《电子商务法》 《网络交易管理办法》
实现服务所需个人信息	账号信息 • 账号 • 口令	仅用于标识网上购物用户和保障账号信息安全。
	收货人信息 • 收货人姓名 • 收货人地址 • 收货人手机号码	仅用于网上购物收货时识别收货人、送达货物和联系收货人，以及完成客服与售后需要。
	第三方支付信息	仅用于用户使用第三方支付方式对网上购物订单付款，通常包括支付时间、支付金额、支付渠道等。
	仅在客服场景下收集： 客服沟通记录和内容 • 通话录音（电话客服） • 聊天消息（在线客服）	仅用于客服处理用户纠纷，具体包括电话客服和在线客服。

表 7 所列个人信息主要针对大众用户购物的普通场景，不包括为跨境电商通关、购买手机号等实名购买情景下需提供的用户身份信息，实名购物场景下通常需要收集用户的证件号码。在一些线上到线下（O2O）的购物场景中，由于需要

判断用户所在的商场、所属的商圈范围等，可能还会收集用户的位置信息，应告知用户并获得用户授权同意。

A.8 短视频

为用户提供短视频服务，包括浏览、搜索、制作、发布短视频和社交互动等功能。该服务类型的最小必要信息如表 8 所示：

表 8 短视频类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	仅对使用信息发布功能的用户收集： 手机号码	《网络安全法》 《移动互联网应用程序信息服务管理规定》 ~~《互联网群组信息服务管理规定》~~
	仅对使用信息发布功能的用户收集： 用户日志信息 • 账号、操作时间、操作类型、网络源地址和目标地址、网络源端口、客户端硬件特征 • 通讯群组名称、昵称、简介、备注、标识 • 用户信息发布、转发、评论记录	《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》
	仅对公众账号信息发布服务使用者收集： 身份认证信息 • 姓名 • 证件类型 • 证件号码	《互联网用户公众账号信息服务管理规定》

类型	个人信息	使用要求/相关法律法规依据
实现服务所需个人信息	账号信息 • 账号 • 口令	仅用于标识短视频用户和保障账号信息安全。
	短视频信息	仅用于对用户短视频进行编辑、美化和发布等。
	关注的账号	仅用于向用户展示和推送关注的账号所发布的短视频。

A.9 快递配送

为用户提供信件、包裹、印刷品等物品的寄递服务，包括寄件、查件、收件等功能。该服务类型的最小必要信息如表 9 所示：

表 9 快递配送类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
实现服务所需个人信息	寄件人基本信息 • 寄件人姓名 • 寄件人地址 • 寄件人联系电话（固定电话或手机号码）	仅用于实现快递寄件和收件功能。
	收件人基本信息 • 收件人姓名 • 收件人地址 • 收件人联系电话（固定电话或手机号码）	
	快递运单号码	仅用于实现快递查件功能和标识快递件。

类型	个人信息	使用要求/相关法律法规依据
	仅在客服场景下收集： 客服沟通记录和内容 • 通话录音（电话客服） • 聊天消息（在线客服）	仅用于客服处理用户纠纷，具体包括电话客服和在线客服。

表 9 所列个人信息主要针对国内快递配送场景，不包括国际快递场景下需提供的收件方身份证件信息和清关信息，以及快递增值业务如代收货款等场景下需提供的支付信息。此外，依据《快递暂行条例》要求，经营快递业务的企业收寄快件，要对寄件人身份进行查验并登记身份信息，但具有快递配送类服务的移动互联网应用程序一般不直接收集相关身份信息。

A.10　餐饮外卖

为用户提供餐饮等外卖信息和外卖服务，包括餐饮配送、到店自取等功能。该服务类型的最小必要信息如表 10 所示：

表 10 餐饮外卖类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	手机号码	《网络安全法》 《移动互联网应用程序信息服务管理规定》
	交易信息	《网络餐饮服务食品安全监督管理办法》 《电子商务法》 《网络交易管理办法》
实现服务所需个人信息	账号信息 • 账号 • 口令	仅用于标识餐饮外卖用户和保障账号信息安全。

类型	个人信息	使用要求/相关法律法规依据
	位置信息	仅用于向用户展示所在位置周边的外卖店铺信息，及便于用户选择外卖收货地址。
	联系人基本信息 • 联系人姓名 • 联系人手机号码 • 联系人地址	仅用于商家和配送员与用户取得联系和配送员送餐，联系人姓名可使用非真实姓名。
	第三方支付信息	仅用于用户使用第三方支付方式对餐饮外卖订单付款，通常包括支付时间、支付金额、支付渠道等。
	仅在客服场景下收集： 客服沟通记录和内容 • 通话录音（电话客服） • 聊天消息（在线客服）	仅用于客服处理用户纠纷，具体包括电话客服和在线客服。

A.11 交通票务

为用户提供交通相关的票务服务，包括票务查询、购买、改签、退票等功能。该服务类型的最小必要信息如表 11 所示：

表 11 交通票务类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	手机号码	《移动互联网应用程序信息服务管理规定》

类型	个人信息	使用要求/相关法律法规依据
	旅客身份证件信息	《公共航空运输企业航空安全保卫规则》 《铁路旅客车票实名制管理办法》 《水路旅客运输实名制管理规定》 ~~《道路旅客运输即客运站管理规定》~~
	交易信息	《电子商务法》 《网络交易管理办法》
实现服务所需个人信息	账号信息 • 账号 • 口令	仅用于标识交通票务用户和保障账号信息安全。
	旅客基本信息 • 旅客姓名 • 旅客类型	仅用于实现用户交通票务和运输服务，包括购票、改签、退票、乘机功能。
	联系人基本信息 • 联系人姓名 • 联系人手机号码	
	行程信息 • 出发地 • 目的地 • 出发时间 • 车次/航班号 • 席别/舱位等级 • 座位号	
	仅在客服场景下收集： 客服沟通记录和内容 • 通话录音（电话客服） • 聊天消息（在线客服）	仅用于客服处理用户纠纷，具体包括电话客服和在线客服。

A.12 婚恋相亲

为用户提供征婚服务，包括异性推荐、相亲牵线等功能。该服务类型的最小必要信息如表 12 所示：

表 12 婚恋相亲类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	手机号码	《网络安全法》 《移动互联网应用程序信息服务管理规定》
实现服务所需个人信息	账号信息 • 账号 • 口令 • 昵称	仅用于标识婚恋相亲用户、保障账号信息安全。
	个人基本资料 • 本人照片 • 性别 • 出生日期 • 所在城市 • 婚姻状况	仅用于异性推荐、相亲牵线等婚恋相亲服务。
	仅在客服场景下收集： 客服沟通记录和内容 • 通话录音（电话客服） • 聊天消息（在线客服）	仅用于客服处理用户纠纷，具体包括电话客服和在线客服。

A.13 求职招聘

为用户提供网上招聘和求职服务，包括职位发布、职位展示、职位搜索、投递简历等功能。该服务类型的最小必要信息如表 13 所示：

表 13 求职招聘类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	手机号码	《网络安全法》 《移动互联网应用程序信息服务管理规定》
实现服务所需个人信息	账号信息 • 账号 • 口令	仅用于标识求职招聘用户，保障账号信息安全。
	求职者基本信息 • 姓名 • 年龄 • 性别 • 健康状况 • 联系邮箱 • 求职意向	仅用于招聘单位识别求职者、岗位需求匹配、招聘单位与求职者联系使用。 求职者民族、视力应为求职者自愿提供，特殊岗位除外。 求职者健康状况不应出现单项健康信息，如是否为乙肝病毒携带者等。
	求职者教育信息 • 学校 • 学历 • 专业 • 毕业时间 • 受教育类型	仅用于求职者简历编辑投递，和招聘单位匹配是否符合岗位需求。
	求职者工作经历信息 • 公司名称 • 职位职务 • 在职时间	
	仅对招聘者用户收集： 招聘者身份信息 • 招聘者姓名 • 招聘者身份证件号码	仅用于对招聘者身份进行认证。

类型	个人信息	使用要求/相关法律法规依据
	仅在客服场景下收集： 客服沟通记录和内容 • 通话录音（电话客服） • 聊天消息（在线客服）	仅用于客服处理用户纠纷，具体包括电话客服和在线客服。

A.14 金融借贷

为用户提供从金融机构进行个人消费贷款服务，包括授信、借款、还款与交易记录等功能，这里的金融机构是指有放贷资质的银行、消费金融公司、小贷公司等在网络上提供借贷服务的机构。该服务类型的最小必要信息如表 14 所示：

表 14 金融借贷类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	手机号码	《移动互联网应用程序信息服务管理规定》
	身份证件信息 • 姓名 • 身份证件种类 • 身份证件号码 • 身份证件有效期限 • 身份证件复印件或影印件	《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》 《互联网金融从业机构反洗钱和反恐怖融资管理办法（试行）》
	仅对借款人收集： 偿付能力 贷款用途	《小额贷款公司网络小额贷款业务风险专项整治实施方案》 《个人贷款管理暂行办法》
实现服务所需个人信息	账号信息 • 账号 • 口令	仅用于标识金融借贷用户和保障账号信息安全。

类型	个人信息	使用要求/相关法律法规依据
	银行账户信息 • 开户行名称 • 银行卡卡号 • 银行卡有效期限 • 银行预留手机号码	仅用于实现银行卡和借贷账号绑卡、银行卡身份认证、借款、还款功能。
	个人信用信息 • 中国人民银行个人信用报告 • 第三方个人信用评分	仅用于对借贷用户的个人信用进行评估，确定授信额度。 个人信用信息须经用户授权查询。
	紧急联系人信息 • 两位常用联系人的联系方式	仅用于金融机构在借贷人逾期不还款时进行催款。 应允许用户在金融借贷应用中手动输入紧急联系人信息，而不应强制读取用户的通讯录。
	借贷交易记录	仅用于确定授信额度、贷款管理、用户借贷历史查询和处理用户纠纷。
	仅在客服场景下收集： 客服沟通记录和内容 • 通话录音（电话客服） • 聊天消息（在线客服）	仅用于客服处理用户纠纷，具体包括电话客服和在线客服。

A.15　房屋租售

为用户提供房源信息、房屋出租服务，包括房源展示、房源搜索、房屋出租等功能。该服务类型的最小必要信息如表 15 所示：

表 15 房屋租售类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	手机号码	《移动互联网应用程序信息服务管理规定》
	交易信息	《电子商务法》 《网络交易管理办法》
实现服务所需个人信息	账号信息 • 账号 • 口令	仅用于标识房屋租售用户和保障账号信息安全。
	租户或业主的身份证件复印件或影印件	仅用于用户线上租房时进行身份验证，以及业主线上发布房源信息、房屋租赁时对身份进行验证。
	业主房产信息	仅用于房源信息发布、房源信息搜索和房屋租赁。
	第三方支付信息	仅用于线上租房交易时使用第三方支付方式完成交易费用支付，通常包括支付时间、支付金额、支付渠道等。
	仅在客服场景下收集： 客服沟通记录和内容 • 通话录音（电话客服） • 聊天消息（在线客服）	仅用于客服处理用户纠纷，具体包括电话客服和在线客服。

如果用户仅浏览房源信息，不需要收集表 15 所列个人信息。表 15 仅列出通过房屋租售类移动互联网应用程序线上收集的个人信息。目前房屋租售服务通常采用线上和线下结合的方式，房源信息和租房大多实现线上服务，而房屋买卖交易仍以线下方式为主，具体收集信息可依据相关政策文件要求。

A.16 二手车交易

二手车交易为用户提供汽车资讯、二手车交易服务，包括车源信息搜索和展示、车辆审核和二手车买卖等功能。该服务类型的最小必要信息如表 16 所示：

表 16 二手车交易类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	手机号码	《移动互联网应用程序信息服务管理规定》
	交易信息	《电子商务法》 《网络交易管理办法》
实现服务所需个人信息	账号信息 • 账号 • 口令	仅用于标识二手车交易用户和保障账号信息安全。
	出售车辆信息 • 车架号 • 车辆审核地址	仅用于网络发布车源前进行现场审核车源时使用，便于审核员到车辆所在地址进行审核。
	购买方信息 • 姓名 • 住址 • 身份证件号码 • 银行卡号码	仅用于二手车购买方的实名制登记、身份验证和完成车辆上户登记、电子签约合同签订等购车流程。 银行卡号码仅用于退还保证金。
	出售方信息 • 姓名 • 身份证件号码 • 驾驶证号 • 车辆行驶证号	仅用于二手车出售方的实名制登记、身份验证和完成车辆上户登记、电子签约合同签订等购车流程。
	第三方支付信息	仅用于二手车交易居间方服务费支付，通常包括支付时间、支付金额、支付渠道等。

类型	个人信息	使用要求/相关法律法规依据
	仅在客服场景下收集： 客服沟通记录和内容 • 通话录音（电话客服） • 聊天消息（在线客服）	仅用于客服处理用户纠纷，具体包括电话客服和在线客服。

表 16 仅列出通过二手车交易类移动互联网应用程序线上收集的个人信息。目前二手车交易服务通常采用线上和线下结合的方式，二手车交易大多已实现电子合同在线签约，车辆审核、车辆上户登记、车辆过户、买卖费用支付等部分环节仍需结合线下进行。

A.17 运动健身

为用户提供运动记录和健康建议服务，包括健身运动管理、健康建议等功能。该服务类型的最小必要信息如表 17 所示：

表 17 运动健身类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
实现服务所需个人信息	账号信息 • 账号 • 口令	账号用于标识运动健身用户和保障账号信息安全。
	位置信息 • 精准定位信息 • 运动轨迹	精确定位信息用于实时确定用户位置和展示用户运动的轨迹。
	个人运动信息	仅用于展示运动过程整体状态信息。

类型	个人信息	使用要求/相关法律法规依据
	基本健康资料 • 性别 • 年龄 • 身高 • 体重	基本健康资料结合个人运动信息，可以更好地给出运动和健康建议。

A.18 问诊挂号

为用户提供在线问诊、在线挂号的医疗服务。该服务类型的最小必要信息如表 18 所示：

表 18 问诊挂号类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	手机号码	《移动互联网应用程序信息服务管理规定》
	交易信息	《电子商务法》 《网络交易管理办法》
实现服务所需个人信息	账号信息 • 账号 • 口令	仅用于标识问诊挂号用户和保障账号信息安全。
	患者身份信息	仅用于在预约挂号时对用户身份进行认证。
	医患沟通信息 • 性别 • 年龄 • 病情描述 • 过往病史 • 是否首诊	仅用于在线问诊时供当前医生判断患者病情。

类型	个人信息	使用要求/相关法律法规依据
	预约挂号信息 • 医院 • 科室	仅用于帮助患者完成预约挂号流程。
	第三方支付信息	仅用于用户使用第三方支付方式对问诊挂号订单付款，通常包括支付时间、支付金额、支付渠道等。

A.19 网页浏览器

为用户提供通过输入网址或站点导航浏览网上信息资源功能的服务，包括网页浏览、文件下载、资源收藏等功能。该服务类型的最小必要信息如表 19 所示：

表 19 网页浏览器类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
实现服务所需个人信息	无	--

A.20 输入法

为用户提供通过键盘、手写、语音等方式输入字符功能的服务。该服务类型的最小必要信息如表 20 所示：

表 20 输入法类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
实现服务所需个人信息	无	--

A.21 安全管理

为用户提供查杀木马病毒、清理恶意插件、修复漏洞、清理优化、骚扰拦截、权限管理等功能。该服务类型的最小必要信息如表 21 所示：

表 21 安全管理类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
实现服务所需个人信息	无	--

为实现识别骚扰、诈骗电话和短信的功能，使用通话记录、短信权限时，宜在智能移动终端中直接处理相关信息。

A.22 旅游服务

为用户提供景点信息、旅游路线规划服务，包括景点展示、景点搜索、旅行路线设计等功能。该服务类型的最小必要信息如表 22 所示：

表 22 旅游服务类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	手机号码	《网络安全法》 《移动互联网应用程序信息服务管理规定》
	交易信息	《电子商务法》 《网络交易管理暂行办法》
实现服务所需个人信息	账号信息 • 账号 • 口令	仅用于标识旅游服务用户和保障账号信息安全。

类型	个人信息	使用要求/相关法律法规依据
	出行人基本信息 • 出行人姓名 • 出行人手机号码 • 出行人证件类型 • 出行人证件号码	仅用于实现用户出游行程预订等服务。
	位置信息	仅用于向用户展示所在位置附近的旅游信息。
	第三方支付信息	仅用于用户使用第三方支付方式对旅游服务订单付款，通常包括支付时间、支付金额、支付渠道等。

表 22 中仅列出通过国内旅游服务类移动互联网应用程序线上收集的个人信息，涉及境外的旅游服务，如办理签证、签注、服务预订等过程，具体收集的个人信息可依据相关政策文件要求和旅游目的地政策等。

A.23 酒店服务

为用户提供酒店信息、酒店预订服务，包括酒店展示、酒店搜索、酒店预订等功能。该服务类型的最小必要信息如表 23 所示：

表 23 酒店服务类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	手机号码	《网络安全法》 《移动互联网应用程序信息服务管理规定》
	住宿人身份证件信息	《旅馆业治安管理条例（征求意见稿）》
	交易信息	《电子商务法》 《网络交易管理暂行办法》
实现服务所需个人信息	账号信息 • 账号 • 口令	仅用于标识酒店预订用户和保障账号信息安全。

类型	个人信息	使用要求/相关法律法规依据
	住宿人和联系人基本信息 • 姓名（住宿人、联系人） • 联系人手机号码	仅用于实现用户预订和入住酒店服务。
	住宿信息 • 入住、退房时间 • 入住酒店名称 • 入住房间号码 • 房型 • 同住人（如有）	仅用于实现用户预订和入住酒店服务。
	位置信息	仅用于向用户展示所在位置附近的酒店住宿信息。
	第三方支付信息	仅用于用户使用第三方支付方式对酒店住宿订单付款，通常包括支付时间、支付金额、支付渠道等。

如果用户仅浏览酒店信息，不需要收集表中所列个人信息。表 23 中仅列出通过酒店预订类移动互联网应用程序线上收集的个人信息。目前酒店入住服务通常采用线上和线下结合的方式，酒店信息展示和预订大多实现线上服务，而酒店入住服务仍以线下方式为主，具体收集信息可依据相关政策文件要求。

A.24 网络游戏

通过互联网、移动通信网等信息网络，为用户提供游戏产品和服务。该服务类型的最小必要信息如表 24 所示：

表 24 网络游戏类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	身份证件信息	《网络游戏管理暂行办法》
实现服务所需个人信息	账号信息 • 账号 • 口令	仅用于标识网络游戏用户和保障账号 信息安全。

类型	个人信息	使用要求/相关法律法规依据
	第三方支付信息	仅用于用户使用第三方支付方式对网络游戏服务订单付款，通常包括支付时间、支付金额、支付渠道等。

根据《儿童个人信息网络保护规定》，App 运营者为征得儿童监护人的有效同意，可能会收集监护人联系方式等信息。

A.25 在线影音

为用户提供在线音视频服务，包括浏览、展示、搜索、播放、下载音视频等功能。该服务类型的最小必要信息如表 25 所示：

表 25 在线影音类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	仅对使用信息发布（包括评论、弹幕等）功能的用户收集： 手机号码	《网络安全法》 《移动互联网应用程序信息服务管理规定》
	仅对公众账号信息发布服务使用者收集： 身份认证信息 • 姓名 • 证件类型 • 证件号码	《互联网用户公众账号信息服务管理规定》
实现服务所需个人信息	账号信息 • 账号 • 口令	仅用于标识在线影音用户和保障账号 信息安全。
	关注的账号	仅用于向用户展示和推送关注的账号所发布的音视频。

类型	个人信息	使用要求/相关法律法规依据
	第三方支付信息	仅用于用户使用第三方支付方式对在线影音服务订单付款，通常包括支付时间、支付金额、支付渠道等。

A.26 儿童教育

为用户提供儿童早教、儿童在线教育服务，包括儿歌教育、童话教育、早教练习等功能。该服务类型的最小必要信息如表 26 所示：

表 26 儿童教育类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	手机号码	《移动互联网应用程序信息服务管理规定》
实现服务所需个人信息	账号信息 • 账号 • 口令	仅用于标识儿童教育用户和保障账号 信息安全。
	儿童基本信息	仅用于提供与儿童年龄等相仿的教育内容，可能包括儿童年级、年龄段、性别等。

根据《儿童个人信息网络保护规定》，App 运营者为征得儿童监护人的有效同意，可能会收集监护人联系方式等信息。

A.27 电子图书

为用户提供读书、听书、漫画等电子图书阅读功能。该服务类型的最小必要信息如表 27 所示：

表 27 电子图书类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	仅对公众账号信息发布服务使用者收集： 身份认证信息 • 姓名 • 证件类型 • 证件号码	《互联网用户公众账号信息服务管理规定》
实现服务所需个人信息	账号信息 • 账号 • 口令	账号用于标识电子图书用户，口令用于保障账号信息安全。

A.28 拍摄美化

为用户提供拍摄照片、摄影、美颜、滤镜、表情包、个性化贴纸等服务。该服务类型的最小必要信息如表 28 所示：

表 28 拍摄美化类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
实现服务所需个人信息	照片或视频信息	仅用于对用户照片或视频进行编辑、美化和保存等。

A.29 应用商店

为用户提供移动互联网应用程序下载、管理等服务。该服务类型的最小必要信息如表 29 所示：

表 29 应用商店类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
实现服务所需个人信息	应用程序列表	仅用于对已安装应用程序进行管理。

A.30　网络直播

为用户提供以视频、音频、图文等形式持续发布实时信息的服务。该服务类型的最小必要信息如表 30 所示：

表 30 网络直播类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	仅对使用信息发布（包括评论、弹幕等）功能的用户收集： 手机号码	《网络安全法》 《移动互联网应用程序信息服务管理规定》
	仅对使用信息发布功能的用户收集： 用户日志信息 • 账号、操作时间、操作类型、网络源地址和目标地址、网络源端口、客户端硬件特征 • 通讯群组名称、昵称、简介、备注、标识 • 用户信息发布、转发、评论记录	《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》

类型	个人信息	使用要求/相关法律法规依据
	仅对互联网直播发布者收集： 身份证件信息	《互联网直播服务管理规定》
实现服务所需个人信息	账号信息 • 账号 • 口令	账号用于标识网络直播用户，口令用于保障账号信息安全。
	第三方支付信息	仅用于用户使用第三方支付方式对网络直播服务订单付款，通常包括支付时间、支付金额、支付渠道等。

2. 《信息安全技术 个人信息告知同意指南（征求意见稿）》10.25 草案与 1.20 版对比

2020 年 1 月 20 日，信安标委在其官网发布了《信息安全技术 个人信息告知同意指南（征求意见稿）》，相较于 2019 年 10 月 TC 260 大会上公布的版本，对比如下，**标准的正文部分没有变动**，附录部分变动较大：

1. 增加个性化推荐、互联网金融、车载和网上购物场景下告知同意的方式。

2019 年 10 月版的附录仅提供了未成年个人信息的告知同意、SDK 收集使用个人信息场景下的告知同意、IoT 场景下的告知同意、公共场合场景下的告知同意，而 2020 年 1 月版则增加了个性化推荐、互联网金融、车载和网上购物场景下告知同意的方式，为现实生活中的常见情景提供更多指导。

2. 对于未成年个人信息的告知同意进行较大变更；

（1） 统一术语为“未成年”

在 2019 年 10 月版中，“未成年”与“儿童”的属于在某些条款是并列时用的，例如告知“未成年人或儿童个人信息的敏感性与应对方法”，2020 年 1 月版删去了儿童，统一术语为“未成年”。

（2） 强调收集未成年信息前的告知时间，完善告知体系

在 2019 年 10 月版中，没有提及告知的时间，而 2020 年 1 月版则强调**收集使用年满 14 周岁的未成年人的个人信息前，宜将个人信息使用规则等信息告知该未成年人或其监护人…；收集不满 14 周岁的未成年人的个人信息前，应将个人信息使用规则等信息告知该未成年人的监护人**。

（3） 变更告知隐私评估报告的前提

在 2019 年 10 月版中，规定幼儿园、学校等采取自动化设备收集未成年个人信息的**可以**说明隐私影响评估报告；而在 2020 年 1 月版则变更为**有必要**时可提供相关的个人信息安全影响评估报告的全文或摘要。

（4） 增加核验监护人身份的方式

2019 年 10 月版仅描述并要求核验个人信息主体是否为不满 14 周岁未成年，而 2020 年 1 月版则区分了不同情形，并核验未成年或监护人的身份。具体而言，若个人信息主体为不满 14 周岁的未成年人，则应当继续采取合理措施核验该未成年人监护人的身份；若个人信息主体为已满 14 周岁的未成年人，则宜继续采取合理措施核验该未成年人监护人的身份。结合验证身份的实际情况，增强要求的合理性。

具体验证监护人身份的方式则区分了仅面向未成年人的应用或终端以及未成年、监护人具有不同终端的情形。具体参见标准的附录 A 2.1 b）项内容。

（5） 丰富对告知、同意方式的描述

2019 年 10 月版仅要求了对于单独面向未成年的终端和应用，以及未成年与监护人存在不同终端和应用的两种情形的告知方式，而 2020 年 1 月版不仅对告知的方式提供了样例，例如发送短信内容的参考，还增加同意的方式的描述，从而为未成年场景下的告知同意提供体系化的指导。

3. 将“SDK 集成者”变更为“宿主 App”

SDK 部分主要变更了术语“SDK 集成者”变更为“宿主 App”，便于读者的阅读，区分 SDK 提供者与宿主 App。

4. 增加智能音箱的告知同意方式

2019 年 10 月版没有规定智能音箱的告知同意方式，在 2020 年 1 月版则填补了粗内容，包括告知同意的方式、告知的时机，为智能音箱这一情景的告知同意提供指导，具体可以参见标准的 C 2.3.1 部分内容。

2020 年 1 月版相较于 2019 年 10 月版在语句顺序以及诸多细节上均有调整，以上仅列明了相较于 2019 年 10 月版的主要变化，具体敬请参见 2020 年 1 月发布的《信息安全技术 个人信息告知同意指南（征求意见稿）》的具体内容。[20]

[20] 作者：孟洁律师团队。

中国首家律师事务所

北京市朝阳区建国路81号华贸中心
1号写字楼15层&20层 邮编: 100025
15 & 20/F Tower 1, China Central Place,
No. 81 Jianguo Road Chaoyang District,
Beijing 100025, China
电话/T. (86 10) 6584 6688
传真/F. (86 10) 6584 6666

上海市黄浦区湖滨路150号企业天地
5号楼26层 邮编: 200021
26F, 5 Corporate Avenue,
No. 150 Hubin Road, Huangpu District,
Shanghai 200021, China
电话/T. (86 21) 2310 8288
传真/F. (86 21) 2310 8299

深圳市南山区铜鼓路39号大冲国际中心
5号楼26层B/C单元 邮编: 518055
Units B/C, 26F, Tower 5,
Dachong International Center, No. 39 Tonggu Road,
Nanshan District, Shenzhen 518055, China
电话/T. (86 755) 8388 5988
传真/F. (86 755) 8388 5987