NEWSLETTER

数据合规

2019 第十期 /总第十期

数据合规时事速递

北京市环球律师事务所

2019 年 10 月 30 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。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、电子商务与广告法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. “两高”发布司法解释 严惩信息网络犯罪

10 月 25 日，最高人民法院、最高人民检察院发布《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》，该解释将于 2019 年 11 月 1 日起施行。

刑法修正案（九）增设内容规定了拒不履行信息网络安全管理义务罪、非法利用信息网络罪和帮助信息网络犯罪活动罪，有力严惩网络犯罪，维护正常网络秩序。但实践中存在定罪量刑标准不易把握、法律适用存在认识分歧等问题。为保障法律正确、统一适用，在公安部等有关部门支持下，最高人民法院会同最高人民检察院制定《解释》，对拒不履行信息网络安全管理义务罪、非法利用信息网络罪和帮助信息网络犯罪活动罪的定罪量刑标准和有关法律适用问题作了全面、系统规定。

亮点一：拒不履行信息网络安全管理义务罪的主体都有谁？

《解释》明确了拒不履行信息网络安全管理义务罪的主体范围，明确“网络服务提供者”包括提供网络接入、域名注册解析等信息网络接入、计算、存储、传输服务，信息发布、搜索引擎、即时通讯、网络支付、网络购物、网络游戏、网络直播等信息网络应用服务，利用信息网络提供的电子政务、通信、交通、金融、教育、医疗等公共服务的单位和个人。

刑法规定，拒不履行信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，有严重情节的，构成犯罪。《解释》明确“监管部门责令采取改正措施”是指网信、电信、公安等依照法律、行政法规的规定承担信息网络安全监管职责的部门，以责令整改通知书或者其他文书形式，责令网络服务提供者采取改正措施。认定“经监管部门责令采取改正措施而拒不改正”，应当综合考虑监管部门责令改正是否具有法律、行政法规依据，改正措施及期限要求是否明确、合理，网络服务提供者是否具有按照要求采取改正措施的能力等因素进行判断。

对于拒不履行信息网络安全管理义务罪的入罪标准，《解释》明确，致使违法信息大量传播的，具体从违法信息数量、传播范围等加以判断；致使用户信息泄露，造成严重后果的，具体从泄露的用户信息数量、后果严重程度等加以判断；致使刑事案件证据灭失，情节严重的，具体从相关证据所涉案件重要程度、造成证据灭失的次数、对刑事诉讼程序的影响等加以判断。

亮点二：非法利用信息网络罪的客观行为方式有哪些？

刑法规定，非法利用信息网络罪在客观方面表现为三种行为方式：设立用于实施诈骗、传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组的；发布有关制作或者销售毒品、枪支、淫秽物品等违禁物品、管制物品或者其他违法犯罪信息的；为实施诈骗等违法犯罪活动发布信息的。《解释》进一步明确，刑法规定的“违法犯罪”，包括犯罪行为和属于刑法分则规定的行为类型但尚未构成犯罪的违法行为；以实施违法犯罪活动为目的而设立或者设立后主要用于实施违法犯罪活动的网站、通讯群组，应当认定为刑法规定的“用于实施诈骗、传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组”；利用信息网络提供信息的链接、截屏、二维码、访问账号密码及其他指引访问服务的，应当认定为刑法规定的“发布信息”。

非法利用信息网络罪以“情节严重”为入罪要件。《解释》规定，假冒国家机关、金融机构名义，设立用于实施违法犯罪活动的网站的，设立用于实施违法犯罪活动的网站，数量达到三个以上或者注册账号数累计达到二千以上的，设立用于实施违法犯罪活动的通讯群组，数量达到五个以上或者群组成员账号数累计达到一千以上的，或者发布有关违法犯罪的信息或者为实施违法犯罪活动发布信息，达到相应标准的，违法所得一万元以上的，二年内曾因非法利用信息网络、帮助信息网络犯罪活动、危害计算机信息系统安全受过行政处罚，又非法利用信息网络的，都属“情节严重”。

亮点三：如何推定帮助信息网络犯罪活动罪的“主观明知”？

刑法规定，构成帮助信息网络犯罪活动罪，要求行为人主观方面“明知他人利用信息网络实施犯罪”。《解释》总结并明确了“主观明知”的推定情形。经监管部门告知后仍然实施有关行为的，接到举报后不履行法定管理职责的，交易价格或者方式明显异常的，提供专门用于违法犯罪的程序、工具或者其他技术支持、帮助的，频繁采用隐蔽上网、加密通信、销毁数据等措施或者使用虚假身份，逃避监管或者规避调查的，为他人逃避监管或者规避调查提供技术支持、帮助的，可认定行为人明知他人利用信息网络实施犯罪。有相反证据的除外。

《解释》还明确了作为帮助信息网络犯罪活动罪入罪要件“情节严重”的认定标准。《解释》规定，为三个以上对象提供帮助的，支付结算金额二十万元以上的，以投放广告等方式提供资金五万元以上的，违法所得一万元以上的，二年内曾因非法利用信息网络、帮助信息网络犯罪活动、危害计算机信息系统安全受过行政处罚，又帮助信息网络犯罪活动的，被帮助对象实施的犯罪造成严重后果的，应当认定为“情节严重”。

亮点四：如何预防网络犯罪罪犯“重操旧业“？

针对网络犯罪一定程度存在的再犯现象，《解释》规定，对拒不履行信息网络安全管理义务、非法利用信息网络、帮助信息网络犯罪活动的罪犯可以依法宣告职业禁止和禁止令。对于实施《解释》规定的犯罪被判处刑罚的，可以根据犯罪情况和预防再犯罪的需要，依法宣告职业禁止；被判处管制、宣告缓刑的，可以根据犯罪情况，依法宣告禁止令。

网络犯罪具有明显的牟利性，为加大财产刑的适用力度，让行为人在经济上得不偿失，进而剥夺其再次实施此类犯罪的经济能力，《解释》规定，应当综合考虑犯罪的危害程度、违法所得数额以及被告人的前科情况、认罪悔罪态度等，依法判处罚金。[1]

《关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》新司法解释全文参见：

http://courtapp.chinacourt.org/fabu-xiangqing-193711.html

2. 《中华人民共和国密码法》明年 1 月 1 日生效

10 月 26 日，十三届全国人大常委会第十四次会议 26 日表决通过密码法，将自 2020 年 1 月 1 日起施行。密码法旨在规范密码应用和管理，促进密码事业发展，保障网络与信息安全，提升密码管理科学化、规范化、法治化水平，是我国密码领域的综合性、基础性法律。

密码法共五章四十四条，重点规范了以下内容：第一章总则部分，规定了本法的立法目的、密码工作的基本原则、领导和管理体制，以及密码发展促进和保障措施。第二章核心密码、普通密码部分，规定了核心密码、普通密码使用要求、安全管理制度以及国家加强核心密码、普通密码工作的一系列特殊保障制度和措施。第三章商用密码部分，规定了商用密码标准化制度、检测认证制度、市场准入管理制度、使用要求、进出口管理制度、电子政务电子认证服务管理制度以及商用密码事中事后监管制度。第四章法律责任部分，规定了违反本法相关规定应当承担的相应的法律后果。第五章附则部分，规定了国家密码管理部门的规章制定权，解放军和

[1] 人民法院报。

武警部队密码立法事宜以及本法的施行日期。

密码法规定，国家对密码实行分类管理。密码分为核心密码、普通密码和商用密码。核心密码、普通密码用于保护国家秘密信息，属于国家秘密。商用密码用于保护不属于国家秘密的信息。公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。

密码法规定，国家加强核心密码、普通密码的科学规划、管理和使用，加强制度建设，完善管理措施，增强密码安全保障能力。国家鼓励商用密码技术的研究开发、学术交流、成果转化和推广应用，健全统一、开放、竞争、有序的商用密码市场体系，鼓励和促进商用密码产业发展。[2]

《中华人民共和国密码法》全文参见：

http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml

3．GB/T 35273《 信息安全技术 个人信息安全规范》最新版征求意见稿

国家标准 GB/T 35273《信息安全技术 个人信息安全规范》于 2019 年 6 月公开向社会征求意见，得到密切关注，截止目前，标准编制组共收到并处理意见约 400 条。基于各单位反馈意见以及 App 违法违规收集使用个人信息专项治理工作实践经验，标准编制组对征求意见稿版本予以补充完善、优化和更新，涉及的主要内容有：

(1) 对部分定义补充完善，优化部分专业词汇描述；

(2) 优化对基本原则的描述；

[2] 新华社。

(3) 对不得强迫接受多项业务功能、授权同意等内容进行更新；

(4) 对个性化展示的使用部分予以更新；

(5) 针对注销难，补充了对注销机制的要求；

(6) 补充了对委托处理、共享、转让等中对受委托者和接受方的管理要求；

(7) 对个人信息共同控制者进行更新；

(8) 其他改动。

最新版征求意见稿与现行生效版本、621 版本的对比请参见本文件第四部分环球评论的第三篇、第四篇文章。

《信息安全技术 个人信息安全规范（征求意见稿）》最新版版全文参见：

https://mp.weixin.qq.com/s/XyJOp2hGujlSKbiLjnpUWA[3]

4. 《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》最新版草案

《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（草案）》于 2019 年 8 月公开向社会征求意见，得到密切关注，其中很多网友以个人身份反馈了意见建议。截止目前，编制组共收到并处理意见 150 余条。基于各单位和个人反馈意见以及 App 违法违规收集使用个人信息专项治理工作实践经验，编制组对草案版本予以补充、优化和更新。更新部分包括：

(1) 对原有第 4 章“管理要求”和“技术要求”进行合并并补充、更新内容；

[3] App 治理工作组。

(2) 对附录 A 中部分服务类型所需最小必要信息进行完善，如网络支付、金融借贷、运动健身等。

(3) 其他改动。

最新版征求意见稿与 8 月版本的对比请参见本文件第四部分环球评论的第五篇文章。

《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）》最新版全文参见：

https://mp.weixin.qq.com/s/y8EUsg9-vDMMinVuHR2ZEA[4]

5．未成年人保护法修订草案增设“网络保护”

10 月 21 日，未成年人保护法修订草案提请十三届全国人大常委会第十四次会议审议，其中专门增设的“网络保护”一章，成为草案的一大亮点，对网络保护的理念、网络环境管理、网络企业责任、网络信息管理、个人网络信息保护、网络沉迷防治、网络欺凌及侵害的预防和应对等作出全面规范，力图实现对未成年人的线上线下全方位保护。

亮点一：关于总原则——保障和引导未成年人安全、合理使用网络

草案明确规定，国家保护未成年人依法使用网络的权利，保障和引导未成年人安全、合理使用网络。家庭和学校应当培养和提高未成年人网络素养，开展网络安全和网络文明教育，提高未成年人安全、合理使用网络的意识和能力，增强未成年人自我保护意识。

亮点二：关于网络不良信息——对上网保护软件强制安装作出规定

针对暴力、色情、涉毒等不良网络信息问题，草案明确提出：国家鼓励和支持有利于未成年人健康成长的网络内容的创作与传播，鼓励和支持专门以未成年人

[4] App 治理工作组。

为服务对象、适合未成年人身心发展特点的网络技术、设备、产品、服务的研发、生产和使用。

草案规定，学校、社区、图书馆、文化馆、青少年宫等场所为未成年人提供的公益性互联网上网服务设施，应当安装未成年人上网保护软件。草案同时规定，网络产品和服务含有可能影响未成年人身心健康信息的，制作、复制、发布、传播该信息的组织和个人应当在信息展示前按照国家有关规定予以提示。

亮点三：关于网络沉迷——要求产品和服务提供者设置时间、权限、消费管理等功能

近年来，未成年人沉迷网游、直播等网络产品和服务不能自拔造成悲剧的事件时有发生。草案规定，网络产品和服务提供者应当避免提供可能诱导未成年人沉迷的内容。网络产品和服务提供者应当设置相应的时间管理、权限管理、消费管理等功能，为父母或者其他监护人预防和干预未成年人沉迷网络提供便利。

在网络游戏方面，草案规定，对未成年人使用网络游戏实行时间管理，具体办法由国务院规定。网络游戏服务提供者应当按照国家有关规定和标准，对游戏产品进行分类，作出提示，并采取技术措施，不得让未成年人接触不适宜其接触的游戏或者游戏功能。

亮点四：关于网络欺凌——不得通过网络以文字、图片、音视频等形式侮辱、诽谤、威胁未成年人

草案规定，任何组织或者个人不得通过网络以文字、图片、音视频等形式侮辱、诽谤、威胁未成年人或者恶意扭曲、损害未成年人形象。发现未成年人遭受上述网络欺凌侵害或者形象遭到恶意扭曲、损害的，受害未成年人的父母或者其他监护人可以要求网络信息服务提供者及时采取删除、屏蔽等措施，停止侵害。

中国互联网络信息中心发布的《2018 年全国未成年人互联网使用情况研究报告》显示，截至 2018 年 7 月 31 日，我国未成年网民规模达 1.69 亿，15.6%的未成年人表示曾遭遇网络暴力。

专家表示，与现实中的欺凌相比，网络欺凌更加难以调查取证，也加大了打击、处罚此类行为的难度。草案作出相关规定，有利于未成年人的父母及时采取措施制止侵害行为。另一方面，有关部门也应对网络平台加强监管，及时发现和惩治网络

欺凌行为。

亮点五：关于个人信息保护——收集未成年人信息需经过未成年人及其父母或者其他监护人同意

草案对未成年人个人网络信息保护作出规定，明确网络产品和服务提供者应当提示未成年人保护其个人信息，并对未成年用户使用其个人信息进行保护性限制。网络产品和服务提供者通过网络收集、使用、保存未成年人个人信息的，应当符合国家有关规定，且经过未成年人及其父母或者其他监护人同意。

亮点六：关于保护责任——明晰未成年人网络保护各方责任

此次未成年人保护法修订草案的重要进步，就在于明确了家长、学校、网络信息服务提供者和政府等各方主体对未成年人网络保护所应承担的责任。

值得注意的是，草案还专门规定，网络产品和服务提供者应当结合本单位提供的未成年人相关服务，建立便捷的举报渠道，通过显著方式公示举报途径和举报方法，配备与服务规模相适应的专职人员，及时受理并处置相关举报。

实践中，当孩子受到网络侵害，家长常常会面临举报途径不畅、处理效果不理想等问题。草案的这一规定，有望督促网络企业提供便捷的举报途径，并通过专业的方式及时解决相关问题，具有较强的现实意义。[5]

6. 全国人大财经委：《互联网金融法》争取列入年度立法计划

10 月 26 日，中国人大网公布了全国人大财经委《关于第十三届全国人民代表大会第二次会议主席团交付审议的代表提出的议案审议结果的报告》，其中显示，“互联网金融法” 争取列入年度立法计划安排审议。

据报告，第十三届全国人民代表大会第二次会议期间，代表提出了关于制定互联网金融法的议案 1 件。全国人大财经委称：议案涉及的立法项目确有立法必要，建议有关部门加强调研起草工作，待草案成熟时，争取列入全国人大常委会年度立

[5] 新华社。

法工作计划安排审议。

最近两年全国两会期间，均有代表呼吁制定互联网金融法。去年两会，全国人大代表阎建国就提出了“关于尽快制定《互联网金融法》的议案”。今年两会，全国人大代表、郑州银行董事长王天宇也提出了关于制定《互联网金融法》的议案，“当下，互联网金融方兴未艾，促进了金融创新，提高了金融资源配置效率，在推动普惠金融发展方面发挥了现有金融机构难以替代的积极作用。但由于缺乏法律法规的约束，互联网金融在快速发展中滋生了一些问题和风险隐患”。

此外，还有代表提出了关于制定快递法的议案，以及关于制定民用无人机管理法的议案、关于制定自动驾驶汽车法的议案。

对于关于制定快递法的议案，全国人大财经委也表示：确有立法必要，建议有关部门加强调研起草工作，待草案成熟时，争取列入全国人大常委会年度立法工作计划安排审议。

而制定民用无人机管理法的议案、自动驾驶汽车法的议案，全国人大财经委则称：建议进一步调研论证，制定完善相关法规政策，解决议案所提问题。[6]

7. 美加州立法禁止在选举期间进行 Deepfake 换脸行为

据外媒报道，日前，美国加州通过一项旨在防止遭修改过的深度伪造(deepfake)视频影响选举的法律。上周，该州州长加文·纽森(Gavin Newsom)签署了《AB 730》。该法案规定，发布任何对政客言行产生虚假、破坏性印象的音频或视频将被视为是一种犯罪行为。

据了解，该法适用于选举期间 60 天内的任何候选人，但也有一些例外，比如新闻媒体以及讽刺或恶搞视频。另外，包含有一个虚假说明的潜在欺骗性视频或音频也将被允许。据悉，这法将于 2023 年终止。

虽然“深度伪造”一词并未出现在立法中，但该法显然针对的就是这一类内容。议员们最近对这种深度伪造视频表现出了非常大的担忧，此前，众议院议长南希·佩

[6] 新京报。

洛西(Nancy Pelosi)的一段讲话视频就遭到了篡改。

与此同时，纽森还签署了一项法禁止未经同意制作色情深度伪造内容的法律。虽然政治上的深度伪造已经成为头条新闻，但数项研究最近发现，深度伪造对准的大部分内容都是色情内容。

不过加州的这一法律引发了人们对言论自由的担忧，加州的美国公民自由联盟等组织就对该法的价值提出了质疑。该组织在一份声明中指出，尽管制定者的本意是好的，但它并不会解决欺骗性政治视频的问题，它只会给选民带来困惑、恶意诉讼和对言论自由的压制。[7]

[7] cnBeta.

二、监管动态

1．习近平：加快推动区块链技术和产业创新发展

10 月 24 日下午，中共中央政治局就区块链技术发展现状和趋势进行第十八次集体学习。习近平总书记在主持学习时强调，要把区块链作为核心技术自主创新的重要突破口，明确主攻方向，加大投入力度，着力攻克一批关键核心技术，加快推动区块链技术和产业创新发展。

习近平总书记的重要讲话，深入浅出地阐明了区块链技术在新技术革新和产业变革中的重要作用，对区块链技术的应用和管理提出了具体要求。总书记的重要讲话，对各部门各地方全面和深刻认识区块链技术发展现状和趋势、提高运用和管理区块链技术的能力必将起到巨大推动作用。[8]

2．欧盟发布 5G 安全风险评估

10 月 11 日，据外电报道，在欧盟委员会和欧洲网络安全局的支持下，欧盟成员国发布了一份欧盟对 5G 网络安全风险的评估报告。报告指出了一些重要的安全挑战，与现有网络的情况相比，这些挑战很可能在 5G 网络中出现或变得更加突出。报道指出，5G 网络的推出预计产生以下影响：

风险一：遭受攻击的风险增加，并且攻击者有更多潜在的切入点

由于 5G 网络越来越基于软件，与重大安全缺陷相关的风险越来越重要，比如供应商内部糟糕的软件开发流程。这还将使威胁行为者更容易恶意地在产品中插入后门，并使其更难被发现。

风险二：对供应商的重度依赖关系带来的风险增加

对单个供应商的重度依赖关系增加了潜在的供应中断风险，例如由于商业破产及其后果导致的供应中断。它还加剧了弱点或漏洞的潜在影响，同时威胁行为者

[8] 央视网。

可能会利用这些弱点，特别是在依赖关系涉及存在高度风险的供应商的情况下。

风险三：对网络可用性和完整性的威胁将成为主要的安全问题

5G 网络预计将成为许多关键 IT 应用的骨干，这些网络的完整性和可用性将成为国家安全的主要问题，从欧盟的角度来看，这也是一个重大的安全挑战。

所有这些挑战共同创造了一个新的安全范式，因此有必要重新评估适用于该领域及其生态系统的当前政策和安全框架，这对于成员国采取必要的缓解措施至关重要。

同时，欧洲网络安全局正在敲定一个与 5G 网络相关的具体威胁分布图，该分布图将更详细地分析报告中涉及的技术内容。[9]

3. 韩国 7 年间个人信息泄露事件达 7428 万件

韩国放送通信委员会近日公开个人信息泄露现状，自 2012 年 8 月运营个人信息泄露报告系统以来，7 年间韩国个人信息泄露事件共计 7428 万件。

在这 7428 万件个人信息泄露案中，给予行政处分的有 6234 万件，征收罚款共计 81.8381 亿韩元。平均每起事件的罚金仅为 131 韩元。2014 年的 745 万起个人信息泄露事件，平均罚款仅 4.6 韩元。放送通信委员会注意到，个人信息泄露事件正急剧增加，从 2017 年的 434 万件增至去年的 931 万件。截至今年 8 月，已有 763 件，预计今年或将超过 1000 万件。

放送通信委员会已收到建议称，对泄露个人信息的企业采取强硬制裁，甚至在立法层面启动保障机制。[10]

[9] TechWeb.
[10] 新民晚报。

三、相关案例

1. 51 信用卡被查，利用爬虫技术抓取数据

“51 信用卡”杭州总部被警方调查近日来引发轩然大波，调查原因是公司外包催债业务涉嫌使用“暴力手段”，而在“暴力手段”背后更深层次的原因则在于，平台利用爬虫技术违规获取了大量用户隐私数据。

被滥用的爬虫技术

所谓爬虫，就是一种程序，它可以像蜘蛛一样，爬到网络的各个角落，自动“搬回”所需要的数据，我们日常使用的搜索引擎，就离不开爬虫采集的数据。同样，目标用户在网上留下的蛛丝马迹，爬虫也可以“爬取”回来。

爬虫又分公开类爬虫和授权类爬虫，公开类爬虫只能爬取各网站公开发布的数据，而授权类爬取可以利用申请者的账号密码登录网站平台。

爬虫本身是无罪的，尤其在互金行业，爬虫曾被广泛使用，它可以通过信息整合、勾勒人群画像，起到防范风险的作用。

问题在于，爬取的信息是否突破了法律的边界。尤其在隐私保护意识薄弱、数据安全存在漏洞的互联网环境中，爬虫技术往往与信息来源违法、过度爬取信息，爬取信息滥用等问题交织。

甚至，有些机构借助爬虫窃取的个人信息，并服务于高利贷、暴力催收等违法行为。

就像此次“51 信用卡”事件中，借贷平台将借款人通讯录、地址定位等信息“交给”催收公司进行“暴力催款”，甚至将借款人其他隐私信息卖给其他平台谋利，让用户备受其他公司“骚扰式营销”的困扰，这些都已经真实发生。

要贷款还是要隐私

“51 信用卡”堪称业内爬虫行业的鼻祖。据公开信息，“51 信用卡”称其“依托于

公司过亿用户和海量大数据，形成了超过 20 个维度的近万个风控变量，提供一站式全流程风险管理服务”。

这样的海量数据从何而来？互联网巨头公司可以基于自身生态链的电商、社交和搜索数据，形成风控产品和数据输出能力，而网贷平台并不具备这样的能力。

答案是“强制授权”

根据“51 信用卡”核心产品“51 人品贷”APP 上的《信息授权服务协议》中的内容来看，用户必须“不可撤销”地授权平台收集从银行卡、邮箱、QQ、电商平台、招聘网站个人简历、微博和微信到其他第三方平台……总计 100 余项涉及个人隐私的数据信息，方可进行贷款申请。

细看条款，一些非常私人的信息，如：QQ 联系人名单、邮箱邮件、手机通话记录和时长、电商平台的收货人地址、信用卡账单、支付平台交易明细都在“51 信用卡”可“收集”的范围之内……除此之外，条款写明“不能保证第三方能做到与平台同等的隐私保护，也不会对第三方的行为及后果承担责任”。这意味着，用户在得到“贷款服务”的同时，必须用自己的“隐私信息”作为代价。

授权不能侵犯个人隐私

早在 2013 年，“51 信用卡”副总经理李俊就透露了获得数据的方式为“读取用户邮箱”。有业界人士猜测，“51 信用卡”或通过不断爬取邮件信息获得用户账户信息，构成了“51 信用卡”的基础数据群。9 月，被警方调查的大数据公司魔蝎科技创始人周江翔，也是 51 信用卡的前高管。已有不少网友爆料，申请贷款后很快收到了“铺天盖地”的各类贷款公司电话，他们猜测，自己的个人信息被卖了。

一般而言，如果是公开的数据，严格遵守网站 Robots 协议，运用爬虫技术就是合理的，而涉及个人隐私数据，采集到公民的姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等个人信息，并将之用于非法途径的，则构成违法行为。而爬取政府机关、银行机构的数据同样违法。

就“51 人品贷”的《信息授权服务协议》中罗列的用户需要被“收集”的信息来看，如 QQ 邮箱邮件、收货地址等数据，事实上就有大部分已经涉及到侵犯个人隐私。

即便数据源得到了用户授权，但是如从非法渠道接入，也是违规的。如果爬取信息，都要获得本人合法授权，即明示、细化的授权，不能概括性授权，否则都是超范围收集个人信息。

相关立法动态

51 信用卡被查的当天，由最高人民法院、最高人民检察院、公安部、司法部等多部门联合制定的《关于办理非法放贷刑事案件若干问题的意见》开始施行。

《意见》明确了对非法放贷行为定罪处罚依据、定罪量刑标准，并明确规定对黑恶势力从事非法放贷活动应当从严惩处，切实维护国家金融市场秩序与社会和谐稳定，防范因非法放贷诱发涉黑涉恶以及其他违法犯罪活动。

在 51 信用卡被调查之前，杭州也已经启动了一轮大数据行业的整肃行动。9 月 6 日，位于杭州的大数据风控平台魔蝎数据科技被警方控制，高管被带走，相关服务瘫痪。

此外，新颜科技、公信宝、同盾科技、百融云创等公司的多名高管也被警方带走调查，同样是因为违规爬取用户信息等问题。

目前，金融行业内正在筹划《个人金融信息保护试行办法》，要求金融机构不得从非法从事个人征信业务活动第三方获取个人金融信息，也不得以“概括性授权”方式取得信息主体对收集、处理、使用和对外提供其个人金融信息的同意。[11]

2. 墨迹 IPO 遭拒，发审委质询数据合规问题

2019 年 10 月 12 日，墨迹科技 IPO 被发审会否决，成为当日四家上会企业中唯一未通过的企业。其中，证监会对墨迹科技的一大质疑点，便是其涉嫌违规收集使用用户数据。

墨迹科技通过自主收集及第三方途径获取用户数据及标签，并利用数据进行商业化变现，公司于 2019 年 7 月 16 日收到 APP 专项治理组发出的《关于 APP 收集使用个人信息相关问题的通知》，APP 专项治理工作组要求公司就收集使用个人

[11] 天下网商。

信息中存在的问题进行整改。

对此，证监会，证监会质问墨迹科技：

(1)获取用户数据及标签的过程及方法，是否对用户有明示提示，用户授权在法律上是否完备，是否明确告知收集信息的范围及使用用途，获取用户数据的手段及方式是否合法合规；

(2)使用用户数据是否合法合规，尤其是商业化变现的合规性，结合相关媒体报道的墨迹天气上传用户隐私等情况，对照《网络安全法》、《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》等法规和司法解释，说明报告期是否存在侵犯用户隐私或数据的的情况，是否存在法律风险或潜在法律风险；

(3)数据获取、使用、处理等过程的内部控制制度及执行情况，对数据安全和个人隐私的保护措施与手段，是否出现过个人信息、隐私泄露事件，是否存在纠纷或潜在纠纷；

(4)日益加强的数据行业监管及个人隐私保护政策对发行人业务的影响及相关应对措施；

(5)针对 APP 专项治理工作组通知指出问题的整改情况及整改效果，是否获得主管部门的认可，是否面临被处罚的风险。[12]

3．酒店强制顾客扫码入住 个人信息采集应坚持“最小化原则”

10 月 15 日，,一些消费者反映,华住集团旗下有的酒店要求住客使用微信扫码办理入住,实际上却是将住客变成自己的“会员”。由此,住客的身份证、家庭地址、生日、邮箱、账号、密码以及银行账户等信息均可能被收集留存。

在扫码购物全面普及的环境下,扫码住酒店看似提供了方便,符合网络时代消费潮流,可住客却在不经意中“被入会”,个人敏感信息被酒店收集、留存。如此操作,很难不让人质疑:其做法是酒店为了采集客户信息数据,挖掘住客的身份背景、经济

[12] 同花顺财经。

能力、消费习惯等,进行精准营销、定制服务所需。这也是很多商家正在做的事。

今年 5 月,国家互联网信息办公室在《数据安全管理办法(征求意见稿)》中强调:仅当用户知悉收集使用规则并明确同意后,网络运营者方可收集个人信息。显然,扫码住酒店“被入会”的做法不属于此例。

无论是理论还是实践,都证明了客户数据的商业价值,为了数据背后广阔的市场空间,很多企业喊出“数据就是生产力”,绞尽脑汁利用各种技术手段采集客户信息,并想方设法深入挖掘、充分利用。然而,技术是一把双刃剑,如果不能善用,就会带来负面效应。现实生活中,已出现很多过度采集客户敏感信息,数据遭到滥用,以及数据保存不当以致泄露或被窃等案例,严重侵犯客户隐私,造成巨大的经济损失和精神伤害。

从本案来看,主角华住集团此前就发生过信息泄露事件。2018 年 8 月,有人在境外网站挂售华住集团 5 亿条会员信息,一度闹得沸沸扬扬,令公众对华住集团的系统防护能力、数据保管水平、内部管理制度产生质疑,亦对其过度采集会员信息表示不满,甚至诱发很多会员主动退会。显然,过度采集客户敏感信息,虽然暂时会给企业带来很多商业利益,但也潜藏着巨大风险,一旦弄不好就会反噬自身,令企业陷入困境。

今年网络安全周期间发布的《2019 年网民网络安全感满意度调查报告》显示,37.4%的网民认为网络个人信息泄露非常多和比较多,58.75%的网民表示个人信息曾遭到侵犯。这一数据表明,超过九成五的网民遇到过网络安全问题。可以说,网络安全问题解决不好,保障不了个人敏感信息安全,必然会影响网络行业甚至整个社会的发展。

因此,我们需要立法明确企业采集个人信息的界限,规定“最小化原则”,即只能采集业务相关的信息数据,避免过度采集。同时,要明确企业保管、使用客户信息数据的责任,对信息泄露进行追责,对违规行为予以严惩。[13]

4．21 个人因侵犯公民个人信息被捕，涉全国 500 万人的信息

日前，宿迁市沭阳县警方在“净网 2019”专项行动中，破获一起涉及全国数百万人的侵犯公民个人信息案件，共抓获犯罪嫌疑人 44 人，成功摧毁犯罪团伙 8 个，

[13] 新华网。

非法获取、买卖公民个人信息约 310 万条，涉案金额达 500 余万元。

今年 2 月初，沭阳县公安局网安大队接群众举报：2018 年 11 月份以来，广东省某贷款公司依托自建的网贷产品，大肆在网络上收集公民个人信息（包含身份信息、联系方式、通话记录、手持身份证照片等），然后再明码标价卖给他人进行非法牟利。

获此线索后，沭阳警方高度重视，抽调精干力量成立专案组，对以李某某、郑某某、郭某某为首的犯罪团伙进行全方位侦查、研判，一张面广量大、层级复杂的侵犯公民个人信息犯罪团伙网络渐渐浮出水面。警方侦查后发现，以李某某为首的广东某贷款公司为“一级源头”，大肆收集公民身份信息，然后以固定价格贩卖给河南郭某某团伙和厦门以郑某某为首的“二级源头”，“二级源头”再将信息低价多次重复出售给以网络贷款公司为代表的“三级源头”。

专案组在充分掌握该犯罪团伙的组织架构、作案手法后，调集 70 余名警力分赴广东、福建、河南、浙江、上海等 10 余个省市开展抓捕工作，共抓获犯罪嫌疑人 44 人，现已采取刑事强制措施 43 人，扣押电脑 41 台，手机 59 部，涉案金额达 500 余万元。

目前，案件正在进一步侦办中。部分网友表示：我们的个人信息早就在“满天飞”了；网友还表示：对个人信息已经泄露表示麻木；许多网友更希望：严惩“信息盗窃贼”。

警方提示，请务必提高自身保护信息安全的防范意识，对身份证复印件、快递面单等包含个人信息的物品进行妥善处置，避免风险 WiFi、钓鱼网址和木马病毒等窃取隐私类的风险，全方位防护信息安全。如发现个人信息已经泄露，要及时采取补救措施以减少损失，同时尽可能收集并保留好相关证据，以备事后维权。[14]

5．Facebook 因人脸识别面临 350 亿美元集体索赔

10 月 20 日,据外媒报道,Facebook 涉嫌滥用面部识别数据的集体诉讼案件出现最新进展。

[14] 江苏网警。

美国第九巡回法院的三名法官驳回了 Facebook 提交的撤销该诉讼案的动议及对原告集体身份验证的上诉。这意味着,除非最高法院介入,Facebook 将不再有机会中止该诉讼案,案件将进入审理程序。

公开信息显示,Facebook 在 2011 年启用了面部识别技术,当时它要求用户识别照片中标记的人是否是他们认识的朋友。

“该诉讼案称,伊利诺伊州市民不同意 Facebook 使用面部识别技术扫描他们上传的照片,而且在 2011 年启用这项技术时,Facebook 并没有告知用户这些数据将保存多久。”有报道称。

法官们说,面部识别软件“侵犯了个人的隐私和利益”。

法庭文件说:“Facebook 的面部识别技术违反了伊利诺伊州的生物特征信息隐私法(BIPA)。违反 BIPA 的规定实际上损害了用户的隐私,或会对他们的隐私构成实质性的威胁。” 而 Facebook 则表示已告知用户已在使用面部识别技术,用户可自由进行选择。

BIPA 对每次过失违规行为处以 1000 美元罚金,对每次故意违规行为处以 5000 美元罚金。该案总共涉及用户为 700 多万,如果最终输掉这场官司,Facebook 面临的总罚款金额最高可能达到 350 亿美元。

Facebook 在一份声明中表示:“Facebook 一直在告诉用户它在使用面部识别技术,并让用户决定是否将这项技术应用到他们身上。我们正在审查我们的选择,并将继续积极为我们自己的做法进行辩护。”

在此前的“全球品牌 100 强”榜单,苹果公司蝉联冠军,谷歌排名第二,而由于 Facebook 被隐私和安全问题所拖累,跌出前十。[15]

[15] 华云网。

6．扎克伯格独闯美国国会接受质询：承认 Libra 存在风险，数据将独立于 Facebook

美国当地时间 10 月 23 日下午 1 时许，Facebook 创始人兼首席执行官扎克伯格出席美国众议院金融服务委员会听证会，该听证会将主要围绕 Libra（天秤币）事宜接受议员的质询。

在听证会开始前，Facebook 先向美国众议院公布了扎克伯格的相关证词。证词中表明，Facebook 将推迟 Libra 的发布，直到完全解决美国监管部门的担忧。

扎克伯格在证词中说，世界上有十多亿人没有银行账户，他们被金融系统拒之门外会给人们的生活带来现实的困难，而天秤币（Libra）就是解决方案之一。扎克伯格指出天秤币项目旨在利用一个安全、低成本且高效的全球转账方式，来促进金融普惠，这将有助于人们摆脱贫困，并将帮助解决社会劳工与企业主的分歧与矛盾。

扎克伯格在证词中还就 Facebook 此前遭受的质疑提出了以下几点回应：Facebook 不会出售个人数据；不会使用个人数据制定借贷决策或创建信用报告；不会与第三方共享借贷决策信息；仅使用 Facebook 上发生的交易信息，来改善其服务，包括广告。但是 Facebook 不会将人们支付账户本身的信息用于广告目的。

以下是听证会现场部分重要内容摘要：

(1) Libra 监管问题

关于议员们担心的 Libra 的监管问题，扎克伯格再次重申，Libra 需要获得包括美国证券交易委员会、金融执法网络等所有监管机构的批准，不会在没有满足所有监管要求的情况下发布 Libra 加密货币，其将通过发布公开声明确认这一点。扎克伯格表示，Libra 并不是要制造一种货币。Libra 是一个国际支付系统，而非银行。Facebook 向监管机构保证，Libra 的数据将与该社交网络分开。

(2) Libra 所有支付成员退出协会问题

针对加入 Libra 协会的支付公司现已全部退出的问题，有议员质疑 Libra 协会难以建立遵守现有反洗钱和银行法保密法等规定的合规制度。

扎克伯格回应称，Libra 协会拥有解决这些问题的专业人士，“我们会和监管机构一起提出解决方案”。针对 7 家公司退出 Libra 协会的市场忧虑，扎克伯格承认 Libra 项目有风险，但认为 Facebook 相关项目并未遭遇危机。扎克伯格同时称，Libra 协会正在招募一名新的独立负责人。

(3) Libra 货币储备问题

听证会上有议员向扎克伯格提问“如何避免 Libra 削弱美元主导地位”，扎克伯格表示：“Libra 储备金将主要是美元，我认为它可以延长美国经济在全球市场的主导地位。”

扎克伯格称，美国金融业相关基础设施已经落后，若要继续保持全球领先地位，美国金融业和金融基础设备需要创新。他同时提及，“在 Libra 白皮书发布后，中国立即公布了央行数字货币。”

(4) Libra 费用问题

针对听证会上议员向扎克伯格质询 Libra 相关的费用问题，扎克伯格回应称，交易免费将会是最终希望达到的目标，但在前期具体的实施过程中会涉及国际间的原则。扎克伯格同时表示，Libra 将主要通过广告的方式实现营收，而不会利用金融数据进行盈利。

(5) 虚假政治广告与新闻服务问题

有议员向扎克伯格提问是否可以通过付费的方式，在 Facebook 上推送错误的选举信息等虚假政治广告，扎克伯格回应称不能。关于政治家所说的信息，Facebook 有一套政策，也有总的原则。针对议员继续询问之前在 Facebook 上没有检查政治广告的行为，扎克伯格回应称“一时还不知道答案”。

听证会上，Facebook 表示将推出支持高质量新闻的新产品，并将举行相关的新闻发布会。Facebook 计划推出一个新闻版面，以汇聚顶级媒体的头条新闻为特色，扎克伯格表示这项服务将采用付费模式。[16]

[16] 界面新闻。

7．Facebook 和 WhatsApp 将必须与英国警察共享用户的加密数据

根据美国和英国之间的一项条约，Facebook 和 WhatsApp 将必须与英国警察共享用户的加密消息，以支持对恐怖主义和恋童癖等严重刑事犯罪嫌疑人的调查。该条约将于下个月签署。

英美两国将不会根据该协议对彼此的公民进行调查。此外，在判处死刑的情况下，该交易迫使美国并非没有从英国公司那里获得使用信息。但是，Facebook 反对这一举动，并在向彭博社的声明中表示，该交易破坏了各地用户的隐私和安全。

美国总统唐纳德·特朗普(Donald Trump)去年签署的《云计算法》(CLOUD Act)或《澄清合法的海外使用数据法》，使执法机构更容易要求在线信息。根据该法案，各机构可以要求存储在任何国家的数据。[17]

8．印度政府要求 Facebook 将帮助解密恐怖分子的数据，称恐怖分子不能要求隐私权

据路透社 10 月 22 日报道，在一场有关社交媒体平台隐私权利的法庭听证会上，印度政府方面以国家安全需要为由，要求 Facebook（脸书）协助其解密网络上的私人消息。

印度总检察长 K.K. Venugopal 向印度最高法院表示，社交媒体公司有责任分享任何涉及国家安全威胁的数据。Venugopal 称："恐怖分子不能要求隐私权。Facebook 和 WhatsApp 说他们不能解密，这个说法是不可以接受的。"

WhatsApp 是 Facebook 旗下的聊天软件，在印度拥有约 4 亿的用户。路透社报道指出，WhatsApp 使用端到端加密来传递文本、照片和视频，不受平台本身或是独立事实审查员的监督。

印度政府方面表示，由于社交媒体不断增长的对个人权利，国家完整、主权与

[17] 极客范。

安全的威胁，计划制定新规则来管理社交媒体。

Facebook 的律师 Mukul Rohtagi 在法庭上回应称，Facebook 没有义务与印度政府共享用户数据。Rohtagi 称，印度当地的法律既没有强制要求公司与政府共享数据，也没有要求公司承担对消息进行解密的责任。

此次印度最高法院针对 Facebook 的审理备受关注，该案件可能会决定日后是否可以强迫包括 Facebook 旗下 WhatsApp 在内的消息服务商、社交媒体公司追踪和披露发件人信息。[18]

9．WhatsApp 被曝漏洞，一张 GIF 动图黑客便可接管账户

近日，Facebook 旗下的消息服务应用 WhatsApp 通过更新程序修复了一个安全漏洞。此前通过该漏洞，黑客能够使用恶意 GIF 入侵该应用程序。

黑客可以通过聊天发送的恶意 GIF 查看用户以往的聊天记录。一旦用户在手机图库中打开一个恶意 GIF 动图，用户在 WhatsApp 中的内容，如聊天记录、用户的个人信息等内容就可能已经被黑客获取。这一漏洞被一名叫 Awakened 的研究员发现并被其公布在了博客中。他表示，使用 Android 8.1 和 9 系统的设备可能更容易受到黑客攻击。

GIF 是黑客经常利用的攻击载荷之一。 5 月，WhatsApp 也曾发现一个漏洞，该漏洞使黑客可以在 WhatsApp 上随意呼叫任何人，并将恶意代码植入其手机，以便查看其个人信息。WhatsApp 随后发布了一个补丁程序解决了这一问题。[19]

10．Google 扫描面部数据遭调查

据《纽约每日新闻》报道，Google 承包商 Randstand 指示员工向包括流浪汉在内的深色皮肤者提供 5 美元的礼品卡。该项目是为了提升 Google Pixel 4 智能手机的数据库，这种手机使用面部识别生物特征测定技术。

[18] 澎湃新闻。
[19] 新浪科技。

Google 声明承认了这个研究项目，并表示多样性对 Pixel 4 的人脸解锁功能来说“至关重要”。声明还称，该公司正在调查有关 Randstand 使用误导策略来说服人们参与面部数据收集项目的说法，Randstand 则未就相关置评请求作出回应。

“我们会定期进行志愿者研究。”Google 发言人说道，“就最近涉及收集人脸样本来进行机器学习训练的研究而言，我们希望在 Pixel 4 的人脸解锁功能中建立公平性，因此样本多样化是至关重要的，这是打造一种包容性产品的重要内容。第二则是安全性，人脸解锁将是一种强大的安全措施，我们希望确保其可保护尽可能多的人。”

然而，这个项目的同意协议规定，Google 有权无限制地保留、使用或共享数据，并可在美国以外的地方处理数据。在这些地方，被收集了数据的目标对象“拥有的权利可能较少”。

“我们正在认真处理这些指控，并对其进行调查。”Google 发言人说道，“这些有关真实性和用户许可的指控违反了我们有关志愿者研究以及我们所提供之培训的规定。”[20]

11．谷歌收集 400 多万 iPhone 用户的数据 绕开 Safari 浏览器的隐私设置

10 月 3 日消息，伦敦上诉法院本周推翻 2018 年时的一项判决，批准就谷歌收集 400 多万 iPhone 用户的数据对谷歌采取法律行动。

原告方表示，Alphabet 旗下谷歌于 2011 年 6 月到 2012 年 2 月绕开了 Safari 浏览器的隐私设置，非法获取了 iPhone 用户浏览互联网的详细数据。

伦敦高等法院于 2018 年 10 月裁定，谷歌在收集、整理和使用浏览器数据过程中扮演的角色存在过错，违反了责任，但原告方并未根据英国的《数据保护法》而遭遇损害。

本案首席律师詹姆斯·奥德纳尔(James Oldnall)表示，上诉法院的裁决“确认了

[20] 新浪科技。

我们的立场，即关于追究企业巨头的责任，代表性行动至关重要”。

这场大型诉讼的代表原告理查德·洛依德(Richard Lloyd)表示，周三的判决“向谷歌和其他大型科技公司发出了非常明确的信号：你们不能凌驾于法律之上”。

他说：“在这个国家，谷歌可以因为滥用个人数据而被追究责任。当企业‘多次并大规模’地侵犯我们的数据保护权益并从中非法获利时，消费者群体可以团结起来，向法院要求企业赔偿。”不过洛依德也表示，他预计法律过程将非常漫长。

谷歌则表示，保护用户的隐私和安全一直是其首要任务。谷歌发言人说：“此案与近 10 年前发生的事件有关，当时我们已经处理过该事件。我们认为，指控不属实，应当予以驳回。”[21]

12．苹果官方回应 Safari 传送数据给 Google 和某科技公司事件

日前 Apple 手机系统 iOS 的 Safari 浏览器私隐政策被发现：“到访网站前，Safari 可能会将网站地址计算出的资料传送予 Google 安全浏览和某科技公司以检查是否为诈骗网站。的文字，引起公众疑虑 Apple 是否会把用户资料交予中国企业手中。

Apple 对此事正式发表回应指出只有区域设定为中国大陆的设备将从某科技公司安全浏览接收诈骗网站列表，且用户到访的网站的 URL 绝对不会传送予安全浏览供应商。

此外，声明指出传输给 Google 和某科技公司的原因为这两个服务器都储存了全球有害及钓鱼网站的列表，为避免用家浏览时不慎到访这些网站，每次登入任何网站前 Safari 都会将装置目的 IP 地址与用家当前的网站 URL 链接地址跟 Google 或 m 欧科技公司传过来的网络例表作比对，确认安全后才会让用户浏览。只有中国的 Safari 用户才会使用某科技公司服务器比对，其他国家及地区都是使用 Google 的。[22]

[21] 新浪科技。
[22] 移动互联网那点事。

13．Adobe 漏洞公开 700 万 Creative Cloud 用户数据

10 月，Adobe 发生严重事故，将 700 万个 Creative Cloud 用户的资料外泄。而 Adobe 方面已经确认事件，提醒用家需要注意欺诈电邮。

问题最初是由安全机构 Comparitech 和安全研究人员 Bob Diachenko 发现，在一个公开的资料库当中包含了大量 Creative Cloud 用户的资料，其中包括电邮地址、帐户建立日期、使用的 Adobe 产品、订阅状态、帐户 ID 和所在地等等。他们向 Adobe 汇报之后，资料库重新被上锁，但据估计已经公开了一星期左右，未知道是否有其他人不当取阅。

虽然被公开的资料库并未包含用户的付款资讯或者帐户密码，不过凭着泄漏的个人资料，攻击者仍然可以进行电邮欺诈等攻击，让目标放下戒心而提供更多的资讯甚至金钱。如果之后有收到 Adobe 所发出的邮件并且要求输入帐户密码或付款详情，必须小心检查是否真的来自 Adobe，如果有不确定的地方就要先向 Adobe 查询，以免遭到欺诈。[23]

[23] 太平洋电脑网。

四、环球评论

1. FTC 首次针对追踪类 App 提起诉讼的官方声明中文翻译

2019 年 10 月 22 日，联邦贸易委员会（Federal Trade Commission，以下简称“FTC”）发布声明，禁止三款监控消费者移动设备位置 App 的开发者继续销售该等 App。FTC 认为三款 App 损害了消费者的隐私权以及移动设备的安全性。

FTC 同时要求 Retina-X Studios，LLC（以下简称“Retina-X”）及其负责人 James N. Johns, Jr. （以下简称“Johns”）删除该等 App 中收集的数据，并在采取足够措施确保 App 仅用于合法的目且安装 App 不会损害设备的安全保护屏障前，禁止推广、销售或上线任何监控类产品。

FTC 消费者保护局局长 Andrew Smith 表示，这是他们首次对所谓的“追踪 App”采取行动，“尽管追踪手机位置可能有合法的理由，但这些 App 却被设计成能在后台偷偷运行并且引发非法和危险的使用。在这种情况下，我们将要求 App 开发者对设计并销售此等危险产品负责。”

FTC 认为，Retina-X 和 Johns 未经移动设备用户的知情或同意，允许 App 的购买者监控安装了该 App 的移动设备地理位置。例如，Retina-X 和 Johns 的“Mobile Spy”的 App 可以监控员工和儿童位置；PhoneSheriff App 和 TeenShield App 可以监控儿童使用的移动设备定位。截至 2018 年 Retina-X 公司停止销售前，三款 App 已经卖出了超过 15000 份。

在安装 App 时，购买者需要绕过移动设备生产商设置的限制。FTC 认为，这将导致设备的安全性降低并可能导致用户失去对移动设备厂家的保修主张。此外，尽管 Retina-X 在其法律政策中声称这些 App 旨在监视员工和儿童，但 Retina-X 并未采取任何措施来确保其 App 仅用于这些目的。

FTC 的诉状中称，每个 App 都向购买者提供了如何在移动设备主屏幕上删除该 App 图标的说明，从而导致使用该设备的使用者不知道该 App 已经安装在该设备上，同时面临因安装该 App 导致的安全漏洞。App 的购买者则能够获取设备使用者的敏感信息，包括用户的身体移动和线上活动轨迹。

此外，Retina-X 和 Johns 未能充分保护从移动设备收集的信息。Retina-X 将其

大部分产品的开发和维护外包给第三方，却未能采用和实施合理的信息安全制度和程序对其 App 进行安全测试或对第三方服务提供商进行监督。

尽管存在诸多隐患，这三个 App 的法律政策均宣称“我们已安全保护您的私人信息”。FTC 诉称，黑客在 2017 年 2 月至 2018 年两次成功访问该公司的云存储账户，并删除某些信息。其中一次黑客访问了 PhoneSheriff 和 TeenShield 两个 App 收集的数据，包括登录用户名、加密的登录密码、短信、GPS 位置、联系人和照片。然而，Retina-X 和 Johns 直到 2017 年 4 月收到记者联络时才知道其系统被黑客入侵。

FTC 认为，Retina-X 和 Johns 违反了《FTC 法案》禁止的不公平和欺骗行为和《儿童在线隐私保护法》（Children’sOnline Privacy Protection Act, 以下简称“COPPA”）。根据 COPPA 的规定，运营商须保护收集的 13 岁以下儿童的信息。Retina-X 收集了儿童的 GPS、短信和其他的个人信息，却没有尽到保护义务，违反了 COPPA 的相关规定。

根据审议的和解协议，Retina-X 和 Johns 必须要求 App 的购买者作出声明，确定 App 仅用于监控儿童或员工，或获得另一名成年人的书面同意。此外，Retina-X 和 Johns 必须确保在移动设备屏幕上设置带有 App 图像和 App 名称的图标。除非由未成年人的父母或法定监护人移除外，任何人均不可删除该图标。同时，Retina-X 和 Johns 不得违反 COPPA 的规定，歪曲他们对隐私和个人信息的保护程度。

此外，FTC 要求 Retina-X 和 Johns 采取措施全面保障其收集的个人信息的隐私和安全，解决 FTC 的诉状中确定的安全问题，并每两年对其信息安全计划进行评估。评估须由第三方完成，评估者须明确支持其结论的证据，并独立进行取样、员工访谈和文件审查。此外，公司须制定一位负责监督信息安全计划的高管，以监督每年的信息安全计划的合规性。最后，该命令收取每两年审核该公司评估的权利。

FTC 以 5-0 的投票同意了 Retina-X 和 Johns 提出的和解协议。FTC 将在《联邦公报》（Federal Register）上发布对和解协议同意的说明，并在发布后的 30 天内接受公众评论。此后，FTC 将决定是否最终做出同意令，并将处理结果发布在 Regulation.gov 网站上。

注：当 FTC 有理由相信某行为已违反法律，且认为对该行为进行诉讼符合公共利益时，FTC 会发起行政诉讼。FTC 最终的发布同意令对未来的行动均有法律

拘束力。违反该指令的行为可能导致最高 42530 美元的民事罚款。[24]

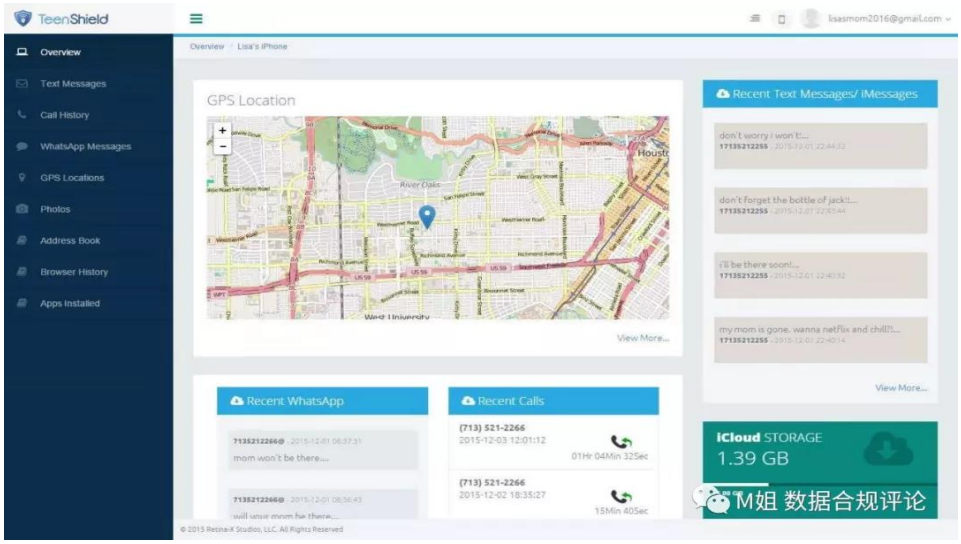
2. 从 FTC 首次两件追踪类 App，谈企业如何防范相关风险

2019 年 10 月 22 日，美国联邦贸易委员会（Federal Trade Commission，以下简称“FTC”）首次针对三款追踪类 App 亮剑，禁止该 App 开发者，Retina-X StudiosLLC 及其所有人 James N. Johns Jr.继续销售该等 App。该等追踪类 App 不仅能够秘密地监控其他人的手机和设备的位置，还能追踪移动设备使用者的通话、短信、图片、物理移动位置和浏览历史记录等信息。目前，FTC 消费者保护机构已于该公司达成和解，FTC 的公告全文翻译参见 FTC“首次针对追踪类 App 提起诉讼”的官方声明中文翻译（DPO 社群出品）。

“追踪类 App”这个名词听起来可能陌生和抽象，然而实际生活中我们都接触过类似的产品或服务，类似的场景如家长可以随时儿童智能电话手表的佩戴者所在位置并进行监控。本文将从介绍追踪类 App 出发，分析追踪类 App 存在的问题与合规难点，以及企业如何保护个人信息、防范风险三个方面进行分析。

一、 追踪类 App 是什么

以本案中受到处罚的、主打父母监控儿童的 App—TeenShield 为例：



[24] 作者：孟洁、张淑怡，https://mp.weixin.qq.com/s/PXrtzKviFodjEGYxICrmkQ。

图片为 TeenShield App 官网展示的 App 功能页面。如左边的导航栏所示，该 App 通过收集相关数据上传至云端，家长可以登录网页随时监控儿童的地理位置、通讯记录、短信内容、WhatsApp 消息内容等，实现**全方位监控**。儿童智能手表的工作原理也是类似的。例如，智能手表的实时监听功能是在手表内置一块 GPS 芯片，而这块芯片会源源不断将孩子（佩戴者）所在的地理位置等通过无线方式发送到云端的服务器，而父母通过手机就能通过访问服务器自动获取到孩子所在的位置。

正如这款 App 的宣传噱头是“帮助父母更好的、全方位监督儿童对移动设备的使用，使儿童远离危险”，这种追踪类 App 之存在的确存在合理之处，特别是对于容易受到网络世界诱惑与沉迷的儿童而言存在一定的保护作用，FTC 的判决也没有完全禁止这类 App 的存在。然而，如何确保该类 App 仅用于正当用途，以及如何对收集来的个人信息加以足够的安全保护措施，是该类 App 面临的两大合规要点。

二、追踪类 App 存在的问题与合规要点

1. 如何确保该类 App 仅用于正当用途

在笔者看来，这个问题是最为首要，也是最难以落地的一个挑战。客观来讲，企业开发 App 后，实际是很难控制该 App 被谁安装、安装在谁的手机上，以及被用于何种用途。即便是 FTC 在公告中给出了相关指导，如要求 App 购买者做出声明，确定 App 仅用于监控儿童或员工，但如何让 App 开发者作出声明，以及怎样的声明是切实有效的，均没有相关指南。面临这种宽泛的规定，使得 Retina-X 公司（即本案被指控的公司）弃步不前。虽然指控的公告是在 2019 年 10 月 22 日做出的，但该公司自 2018 年云存储被黑客入侵的消息被曝出后不久该公司便关停了此服务，至今仍未重启该项目。

2. 是否对收集来的信息加以足够的保护措施

FTC 的公告中的很大篇幅均在说明 Retina-X 公司对收集来的数据没有尽到足够的安全保护义务，具体表现为没有采用和实施合理的信息安全制度和程序对其 App 进行安全测试，没有对负责产品开发和维护的第三方服务提供商进行监督，包括没有进行安全评估与审计。

我国的相关法律法规、国家标准也有类似的要求。就对收集的个人信息进行安全保护而言，我国**《网络安全法》**第 21 条规定，网络运营者应当按照网络安全等

级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；（四）采取数据分类、重要数据备份和加密等措施……；**《数据安全管理办法（征求意见稿）》**第 6 条的规定，网络运营者应当按照有关法律、行政法规的规定，参照国家网络安全标准，履行数据安全保护义务，建立数据安全管理责任和评价考核制度，制定数据安全计划，实施数据安全技术防护……。针对委托第三方进行管理的情形，**《信息安全技术个人信息安全规范（征求意见稿）》（10.22 版）**第 8.1 条 d）款规定，个人信息控制者应对受委托者进行监督，方式包括对受委托者进行审计等。

这一个要求相较于上一条更具实践解决性，企业如若遵守了相关规范，则在一定程度上证明对个人信息尽到了安全保护义务，降低相关风险。

三、企业如何做好合规措施，提前防范相关风险

鉴于本案的借鉴意义，我们建议开发追踪类 App 的企业采取以下措施规避相关风险：

1. 尽可能地规避 App 用于不法用途

例如，在用户下载 App，每次安装在不同的手机上时均需要签署电子手写的同意书，明确仅用于监控儿童的用途，以此尽可能地证明企业已采取措施避免 App 用于不法用途，并在接受到用户举报时立即采取必要措施，例如切断相关人员对该用户的访问，避免损害扩大。

2. 实施足够的安全保护措施，保障收集的个人信息的安全性

本案中的 FTC 举证 Retina-X 未尽安保义务的证据之一为黑客在 2017 年 2 月至 2018 年两次成功访问该公司的云存储账户，并删除某些信息，故建议企业应根据有关国家网络安全标准的要求，如有需要实时更新必要的管理和技术措施，防止个人信息的泄漏、损毁、丢失、篡改等。

3. 定期对采取的安全措施的有效性进行评估

建议企业对安全措施有效性进行审计，必要时开展网络安全等级保护评估、获

取网络安全认证证书，如 ISO27001、ISO27018、ISO22301 等。

4. **存在委托第三方处理的，应确保第三方具有足够的数据安全能力**

对于委托第三方进行处理的情形，建议企业对委托行为进行个人信息安全影响评估，确保受委托者达到相应的数据安全能力。如果受托方是新的供应商，那么需要通过合规 checklist 对供应商进行更为严格的审查，逐一判断能力资质等是否符合公司的隐私保护要求。并且，需要通过合同或者定期审计的方式对受委托者进行审计与监督，一旦发现或得知受委托者没有履行个人信息安全保护责任的，应立即要求受托者停止相关行为，并采取有效补救措施控制或消除个人信息面临的安全风险。

5. **指定负责人实时监督信息安全计划的合规性**

目前我国有关个人保护的立法仍处于探索和发展的状态，建议达到一定规模的企业任命个人信息保护负责人和个人信息保护工作机构（至少成立协调机构），除对企业产品或服务上线发布前进行检测、开展个人信息影响安全评估外，应实时关注有关个人信息保护的立法与监管动态，当有新的法律法规或者国家标准出台时，应及时审查企业采取措施的合规状况，更新合规举措。如果 App 是针对特殊类型主体所开发的，或者收集的信息是特殊敏感的个人信息，还需要针对性地了解与该特殊类型主体相关的以及如何保护个人敏感信息的特殊规定。如果 App 还向其他国家发行的，还需要及时了解境外所涉及法域的法律、法规。[25]

3. 《信息安全技术 个人信息安全规范》最新版征求意见稿与 621 版本的比照

全国信息安全标准化技术委员会于 2019 年 10 月 24 日发布了《个人信息安全规范（征求意见稿 10.22 版）》，我们详细比对了《个人信息安全规范（征求意见稿 10.22 版》与《个人信息安全规范（征求意见稿 6.21 版）》，以表格的方式列出了两个版本中相应条款存在的主要区别，并以红色的字体标识。详细内容参见下表：[26]

[25] 作者：孟洁律师团队，https://mp.weixin.qq.com/s/xgsBTDM0jBKUJyvkgfXB0g。
[26] 作者：孟洁律师团队，https://mp.weixin.qq.com/s/T2HWA1KTXF94VyWypJ_Rpw。

	6 月 21 日版	10 月 22 日版
个人信息的定义		新增： 注 3：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，例如用户画像或特征标签，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，属于个人信息。
个人敏感信息的定义		新增： 注 3：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，如一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的，属于个人敏感信息。
个人信息主体的定义	个人信息所标识的自然人。	个人信息所标识或者关联的自然人。
明示同意的定义	个人信息主体通过书面主动声明或自主作出肯定性动作，对其个人信息进行特定处理作出明确授权的行为。 注：肯定性动作包括个人信息主体主动作出声明（电子或纸质形式）、主动勾选、主动点击“同意”、“注册”、“发送”、“拨打”、主动填写或提供等。	个人信息主体通过书面、口头等方式主动作出纸质或电子形式的声明，或者自主作出肯定性动作，对其个人信息进行特定处理作出明确授权的行为。 注：肯定性动作包括个人信息主体主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。
授权同意的定义	未作出。	新增： 个人信息主体对其个人信息进行特定处理作出明确授权的行为，包括通过积极的行为作出授权（即明示同意），或者通过消极的不作为而作出授权（例如信息采集区域内的个人信息主体在被告知信息收集行为后没有离开该区域）。
匿名化的定义	通过对个人信息的技术处理，使得个人信息主体无法被识别，且处理后的信息不能被复原的过程。	通过对个人信息的技术处理，使得个人信息主体无法被识别或者关

	6 月 21 日版	10 月 22 日版
		联，且处理后的信息不能被复原的过程。
去标识化的定义	通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别个人信息主体的过程。	通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别或者关联个人信息主体的过程。
个人信息安全基本原则	个人信息控制者开展个人信息处理活动，应遵循以下基本原则： b) 目的明确原则——具有合法、正当、必要、明确的个人信息处理目的。 d) 最少够用原则——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。目的达成后，应及时删除个人信息。	个人信息控制者开展个人信息处理活动应遵循合法、正当、必要的原则，具体包括： b) 目的明确——具有明确、清晰、具体的个人信息处理目的。 d) 最小必要——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。目的达成后，应及时删除个人信息。
收集个人信息的合法性	对个人信息控制者的要求包括： b) 不应隐瞒产品或服务所具有的收集个人信息的功能；	对个人信息控制者的要求包括： b) 不应隐瞒产品或服务所具有的收集个人信息的业务功能； 新增：e) 不应大规模收集我国公民的种族、民族、政治观点、宗教信仰等个人敏感信息。
不强迫接受多项业务功能	a) 不应通过捆绑产品或服务各项业务功能的方式，要求个人信息主体一次性接受并授权同意各项业务功能收集个人信息的请求。 b) 应把个人信息主体自主选择行为，如主动点击、勾选、填写等，作为产品或服务的特定业务功能的开启条件。个人信息控制者应仅个人信息主体开启该业务功能且符合本标准 5.4 相关要求后，开始收集个人信息；	a）不应通过捆绑产品或服务各项业务功能的方式，要求个人信息主体一次性接受并授权同意其未申请或使用的业务功能收集个人信息的请求。 b) 应把个人信息主体自主作出的肯定性动作，如主动点击、勾选、填写等，作为产品或服务的特定业务功能的开启条件。个人信息控制者应仅在个人信息主体开启该业务功能后，开始收集个人信息； 新增：f）不应以改善服务质量、提升个人信息主体体验、研发新产品、增强安全性等为由，强迫要求个人信息主体同意收集个人信息。

	6 月 21 日版	10 月 22 日版
收集个人信息时的授权同意	b) 收集个人敏感信息前，应征得个人信息主体的明示同意，并应确保个人信息主体的明示同意是其在完全知情的基础上自主给出的、具体的、清晰明确的意愿表示； d）2）应了解个人信息提供方已获得的个人信息处理的授权同意范围，包括使用目的，个人信息主体是否授权同意转让、共享、公开披露等。本组织开展业务所需进行的个人信息处理活动超出该授权同意范围的，应在获取个人信息后的合理期限内或处理个人信息前，征得个人信息主体的明示同意。	b）收集个人敏感信息前，应征得个人信息主体的明示同意，并应确保个人信息主体的明示同意是其在理解收集目的和相关处理规则的基础上自主给出的、具体的、清晰明确的意愿表示； d）2）应了解个人信息提供方已获得的个人信息处理的授权同意范围，包括使用目的，个人信息主体是否授权同意转让、共享、公开披露、删除等； 3）如开展业务所需进行的个人信息处理活动超出已获得的授权同意范围的，应在获取个人信息后的合理期限内或处理个人信息前，征得个人信息主体的明示同意，或通过个人信息提供方征得个人信息主体的明示同意。
去标识化处理	收集个人信息后，个人信息控制者宜立即进行去标识化处理，并采取技术和管理方面的措施，将去标识化后的信息与可用于恢复识别个人的信息分开存储。	收集个人信息后，个人信息控制者宜立即进行去标识化处理，并采取技术和管理方面的措施，将可用于恢复识别个人的信息与去标识化后的信息分开存储并加强访问和使用的权限管理。
个人敏感信息的存储和传输	b) 存储个人生物识别信息时，应采用技术措施确保信息安全后再进行存储，例如将个人生物识别信息的原始信息和摘要分开存储，或仅存储摘要信息。	b）存储个人生物识别信息时，应采用技术措施确保信息安全后再进行存储，例如将个人生物识别信息的原始信息和摘要分开存储，或仅收集、存储、使用摘要信息。
个性化展示及退出	对个人信息控制者的要求包括： a) 在向个人信息主体推送新闻信息服务的过程中使用个性化展示的，应： 1) 显著区分个性化推送服务，如标明“个性化展示”或“定推”等字样； 2) 为个人信息主体提供简单直观的退出或关闭个性化展示模式的选项。	对个人信息控制者的要求包括： a) 在向个人信息主体提供业务功能的过程中使用个性化展示的，应显著区分个性化展示的内容和非个性化展示的内容；注：显著区分的方式包括但不限于：标明“定推”等字样，或通过不同的栏目、版块、页面分别展示等。 b) 在向个人信息主体提供电子商务服务的过程中，根据消费者的

	6 月 21 日版	10 月 22 日版
	b) 电子商务经营者根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务搜索结果的个性化展示的，应当同时向该消费者提供不针对其个人特征的选项； 注：基于用户所选择的特定位置进行展示、搜索结果排序，且不因用户身份不同展示不一样的内容和搜索结果排序，则属于不针对其个人特征的选项。 c) 在向个人信息主体提供业务功能的过程中使用个性化展示的，宜： 1) 建立个人信息主体对个性化展示所依赖的个人信息（如标签、画像维度等）的自主控制机制，保障个人信息主体调控个性化展示相关程度的能力； 2) 当个人信息主体选择退出个性化展示模式时，向个人信息主体提供删除或匿名化定向推送活动所基于的个人信息的选项。	兴趣爱好、消费习惯等特征向其提供商品或者服务搜索结果的个性化展示的，应当同时向该消费者提供不针对其个人特征的选项；注：基于个人信息主体所选择的特定位置进行展示、搜索结果排序，且不因个人信息主体 身份不同展示不一样的内容和搜索结果排序，则属于不针对其个人特征的选项。 c) 在向个人信息主体推送新闻信息服务的过程中使用个性化展示的，应： 1) 为个人信息主体提供简单直观的退出或关闭个性化展示模式的选项； 2) 当个人信息主体选择退出或关闭个性化展示模式时，向个人信息主体提供删除或匿名化定向推送活动所基于的个人信息的选项。 d) 在向个人信息主体提供业务功能的过程中使用个性化展示的，宜建立个人信息主体对个性化展示所依赖的个人信息（如标签、画像维度等）的自主控制机制，保障个人信息主体调控个性化展示相关程度的能力。
信息系统自动决策机制的使用	c) 向个人信息主体提供针对自动决策结果的申诉渠道，并对自动决策结果进行人工复核。	c）向个人信息主体提供针对自动决策结果的投诉渠道，支持通过人工方式对个人信息主体投诉情形进行复核。
个人信息主体注销账户		对个人信息控制者的要求包括： 新增：b) 宜直接设置便捷的注销功能交互式页面，及时响应个人信息主体注销请求； c) 受理注销账号请求后，需要人工处理的，应在承诺时限内（原则上不超过十五天）完成核查和处理；

	6 月 21 日版	10 月 22 日版
		d) 注销过程进行身份核验需要个人信息主体重新提供的个人信息不应多于注册、使用等服务环节收集的个人信息； e) 注销过程不应设置不合理的条件或提出额外要求增加个人信息主体义务，如注销单个账户视同注销多个产品或服务，要求个人信息主体填写精确的历史操作记录作为必要注销条件等； f) 注销账户的过程需收集个人敏感信息核验身份时，应明确对收集个人敏感信息后的处理措施，如达成目的后立即删除或匿名化处理等； 注：因法律规规定需要留存的个人信息应妥善保管，不能将其再次应用于业务场景。
响应个人信息主体请求	b) 宜直接在产品或服务提供的功能界面中（例如应用程序可设置专门的选项、功能、界面等）设置相应的机制，便于个人信息主体在线行使其访问、更正、删除、撤回授权同意、注销账户等权利；	b）宜直接在产品或服务提供的界面中设置专门的功能或选项，便于个人信息主体在线行使其访问、更正、删除、撤回授权同意、注销账户等权利； 新增：如决定不响应个人信息主体的请求，应向个人信息主体告知该决定的理由，并向个人信息主体提供投诉的途径。
委托处理		新增：f）个人信息控制者得知或者发现受委托者未按照委托要求处理个人信息或未能有效履行个人信息安全保护责任的，应立即要求受托者停止相关行为，且采取或要求受委托者采取有效补救措施（例如更改口令、回收权限、断开网络连接等）控制或消除个人信息面临的安全风险。必要时个人信息控制者应终止与受委托者的业务关系，并要求受委托者及时删除从个人信息控制者获得的个人信息。

	6 月 21 日版	10 月 22 日版
个人信息共享转让	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； e) 承担因共享、转让个人信息对个人信息主体合法权益造成损害的相应责任；	b）向个人信息主体告知共享、转让个人信息的目的、数据接收方的类型以及可能产生的后果，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或者关联个人信息主体的除外； g）因共享、转让个人信息发生安全事件而对个人信息主体合法权益造成损害的，个人信息控制者应承担相应的责任； 新增：d）通过合同等方式规定数据接收方的责任和义务； f）个人信息控制者发现数据接收方违反法律法规要求或双方约定处理个人信息的，应立即要求数据接收方停止相关行为，且采取或要求数据接收方采取有效补救措施（例如更改口令、回收权限、断开网络连接等）控制或消除个人信息面临的安全风险；必要时个人信息控制者应解除与数据接收方的业务关系，并要求数据接收方及时删除从个人信息控制者获得的个人信息。
收购、兼并、重组、破产时的个人信息转让		新增：c）如破产且无承接方的，对数据做删除处理。
个人信息公开披露		新增：g）不应公开披露我国公民的种族、民族、政治观点、宗教信仰等个人敏感数据的分析结果。
共同个人信息控制者	当个人信息控制者与第三方为共同个人信息控制者时（例如服务平台与平台上的签约商家），个人信息控制者应通过合同等形式与第三方共同确定应满足的个人信息安全要求，以及在个人信息安全方面自身	对个人信息控制者的要求包括： a) 当个人信息控制者与第三方为共同个人信息控制者时，个人信息控制者应通过合同等形式与第三方共同确定应满足的个人信息安全要求，以及在个人信息安全方面

	6 月 21 日版	10 月 22 日版
	和第三方应分别承担的责任和义务,并向个人信息主体明确告知。	自身和第三方应分别承担的责任和义务,并向个人信息主体明确告知。 新增：b) 如未向个人信息主体明确告知第三方身份，以及在个人信息安全方面自身和第三方应分别承担的责任和义务，个人信息控制者应承担因第三方引起的个人信息安全责任。
第三方接入管理	g) 应督促和监督第三方产品或服务提供者加强个人信息安全管理，发现第三方产品或服务没有落实安全管理要求和责任的，应及时督促整改，必要时停止接入；	g）应督促第三方产品或服务提供者加强个人信息安全管理，发现第三方产品或服务没有落实安全管理要求和责任的，应及时督促整改，必要时停止接入；
个人信息跨境传输	在中华人民共和国境内运营中收集和产生的个人信息向境外提供的，个人信息控制者应符合国家网信部门会同国务院有关部门制定的办法和相关标准的要求。	在中华人民共和国境内运营中收集和产生的个人信息向境外提供的，个人信息控制者应遵循国家相关规定和相关标准的要求。
个人信息安全事件应急处置和报告	c）4）个人信息泄露事件可能会给个人信息主体带来较大影响的，如个人敏感信息的泄露，照本标准 9.2 的要求实施安全事件的告知。	c）4）个人信息泄露事件可能会给个人信息主体的合法权益带来严重危害的，如个人敏感信息的泄露，照本标准 9.2 的要求实施安全事件的告知。
明确责任部门与人员	d) 个人信息保护负责人和个人信息保护工作机构的职责应包括但不限于： 5) 开展个人信息安全影响评估，提出个人信息保护的对策建议；	c) 满足以下条件之一的组织，应设立专职的个人信息保护负责人和个人信息保护工作机构，负责个人信息安全工作： 新增：3) 处理个人敏感信息的。 d）个人信息保护负责人和个人信息保护工作机构的职责应包括但不限于： 5）开展个人信息安全影响评估，提出个人信息保护的对策建议，督促整改安全隐患；
数据安全能力	个人信息控制者应根据有关国家标准的要求，建立适当的数据安全能力，落实必要的管理和技术措施，防止个人信息的泄漏、损毁、丢失。	个人信息控制者应根据有关国家标准的要求，建立适当的数据安全能力，落实必要的管理和技术措

	6 月 21 日版	10 月 22 日版
		施，防止个人信息的泄漏、损毁、丢失、篡改。
人员管理和培训	a) 应与从事个人信息处理岗位上的相关人员签署保密协议，对大量接触个人敏感信息的人员进行背景审查；	a）应与从事个人信息处理岗位上的相关人员签署保密协议，对大量接触个人敏感信息的人员进行背景审查，以了解其犯罪记录、诚信状况等；
安全审计	b) 应建立自动化审计系统，监测记录个人信息处理活动；	b）应采取建立自动化审计系统等方式，监测记录个人信息处理活动； 新增：f）审计记录和留存时间应符合法律法规的要求。

4. 《信息安全技术 个人信息安全规范》现行生效版、621 版、1022 版附录比对

全国《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（草案）》于 2019 年 8 月公开向社会征求意见，得到密切关注。10 月 24 日编制组发布更新版草案，，我们已于 10 月 24 日发布了最新版本与 6 月 21 日版本的主要改动方向，此次将就附录部分的主要改动点，对现行生效版本、6 月 21 日版本和 10 月 22 日版本进行对比。[27]

	现行生效版本	6 月 21 日版本	10 月 22 日版本
附录 A 网络身份标识信息	系统账号、IP 地址、邮箱地址及与前述有关的密码、口令、口令保护答案、用户个人数字证书等	较现行生效版本基本无变化。	个人信息主体账号、IP 地址、邮箱地址及与前述有关的密码、口令、口令保护答案、个人信息主体个人数字证书等

[27] 作者：孟洁律师团队，https://mp.weixin.qq.com/s/ZtLoA3sW-LU23zIERE6l9w。

	现行生效版本	6 月 21 日版本	10 月 22 日版本
附录 B 网络身份标识信息	系统账号、邮箱地址及与前述有关的密码、口令、口令保护答案、用户个人数字证书等	个人信息主体账号、口令、口令保护答案、用户个人数字证书等的组合	较 6 月 21 日版本版本基本无变化。
附录 B 其他信息	个人电话号码、性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等	性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、群组列表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等	较 6 月 21 日版本版本基本无变化。
附录 C	/	C.1 区分基本业务功能和扩展业务功能 保障个人信息主体选择同意的权利，首先需划分产品或服务的基本业务功能和扩展业务功能，划分的方法如下： a) 应根据个人信息主体选择、使用所提供产品或服务的根本期待和最主要的需求，划定产品或服务的基本业务功能； 注 1：个人信息主体之所以识别或挑选某项产品或服务，主要依据个人信息控制者对所提供产品或服务开展的市场推广和商业定位、产品或服务本身的名称、在应用商店中的描述、所属的应用类型等因素。因此，个人信息控制	较 6 月 21 日版本版本基本无变化。

	现行生效版本	6 月 21 日版本	10 月 22 日版本
		者应根据一般用户对上述因素的最可能的认识和理解，而非自身想法来确定用户的主要需求和期待来划定基本业务功能。一般来说，如果产品或服务不提供基本业务功能，个人信息主体将不会选择使用该产品或服务。 注 2：随着产品或服务的迭代、拓展、升级等，基本业务功能可能需要随之重新划分。个人信息控制者仍应根据一般用户最可能的认识和理解，来重新划定基本业务功能。但个人信息控制者不应短时间内大范围改变基本业务功能和扩展业务功能的划分。在重新划分后，个人信息控制者应再次告知并征得个人信息主体对基本业务功能收集、使用其个人信息的明示同意。 b) 不应将改善服务质量、提升用户体验、研发新产品单独作为基本业务功能； c) 将产品或服务所提供的基本业务功能之外的其他功能，划定为扩展业务功能。	

	现行生效版本	6 月 21 日版本	10 月 22 日版本
	/	C.2 基本业务功能的告知和明示同意 基本业务功能的告知和明示同意的实现方法如下： a) 在基本业务功能开启前（如个人信息主体初始安装、首次使用、注册账号等），应通过交互界面或设计（如弹窗、文字说明、填写框、提示条、提示音等形式），向个人信息主体告知基本业务功能所必要收集的个人信息类型，以及个人信息主体拒绝提供或拒绝同意收集将带来的影响，并通过个人信息主体对信息收集主动作出肯定性动作（如勾选、点击“同意”或“下一步”等）征得其明示同意； 注：当产品或服务所提供的基本业务功能无需一次性全部开启时，应根据个人信息主体的具体使用行为逐步开启基本业务功能，并即时完成本条 a)的告知要求。 b) 个人信息主体不同意收集基本业务功能所必要收集的个人信息的，个人信息控制者可拒绝向个人	较 6 月 21 日版本版本基本无变化。

	现行生效版本	6 月 21 日版本	10 月 22 日版本
		信息主体提供该业务功能； c) 本条 a）所要求的交互界面或设计应方便个人信息主体再次访问及更改其同意的范围。 注：上述要求的实现方式可参考附录 C.4。	
	/	C.3 扩展业务功能的告知和明示同意 扩展业务功能的告知和明示同意的实现方法如下： a) 在扩展业务功能首次使用前，应通过交互界面或设计（如弹窗、文字说明、填写框、提示条、提示音等形式），向个人信息主体逐一告知所提供扩展业务功能及所必要收集的个人信息，并允许个人信息主体对扩展业务功能逐项选择同意； b) 个人信息主体不同意收集扩展业务功能所必要收集的个人信息的，个人信息控制者不应反复征求个人信息主体的同意。除非个人信息主体主动选择开启扩展功能，在 24 小时内向用户征求同意的次数不应超过一次；	较 6 月 21 日版本版本基本无变化。

	现行生效版本	6 月 21 日版本	10 月 22 日版本
		c) 个人信息主体不同意收集扩展业务功能所必要收集的个人信息的，不应拒绝提供基本业务功能或降低基本业务功能的服务质量； d) 本条 a）所要求的交互界面或设计应方便个人信息主体再次访问及更改其同意的范围。 注：上述要求的实现方式可参考附录 C.4。	
附录 C	本附录给出了向个人信息主体就个人敏感信息的收集、使用，以及个人信息的共享、转让、公开披露等事项征求授权同意的实现方法。个人信息控制者可参考以下模板设计功能界面，保障个人信息主体能充分行使其选择同意的权利。 该功能界面应在个人信息控制者开始收集个人敏感信息前，如产品安装过程中，或个人信息主体首次使用产品或服务时，或个人信息主体注册账号时，由个人信息控制者主动向个人信息主体提供。如以填写纸质材料收集个人敏感信息的，个人信息控制者可以参考以下模板内容设计表格，以保障个人信	C.4 交互式功能界面设计 个人信息控制者可参考以下模板设计交互式功能界面，保障个人信息主体能充分行使其选择同意的权利。 该功能界面应在个人信息控制者开始收集个人信息前，如产品安装过程中，或个人信息主体首次使用产品或服务时，或个人信息主体注册账号时，由个人信息控制者主动向个人信息主体提供。如以填写纸质材料收集个人信息的，个人信息控制者可以参考以下模板内容设计表格，以保障个人信息主体能行使选择同意的权利。	较 6 月 21 日版本版本基本无变化。

	现行生效版本	6 月 21 日版本	10 月 22 日版本
	息主体能行使选择同意的权利。		
附录 C 交互式功能界面设计说明	1、 为向个人信息主体清晰展示收集个人敏感信息的目的、种类等，并分情形征得个人信息主体同意。建议个人信息控制者采用分阶段、分窗口、分屏幕等方式向个人信息主体展示左侧模 板中的功能界面。	1、为向个人信息主体清晰展示收集个人信息的目的、种类等，并分情形征得个人信息主体同意。建议个人信息控制者采用分阶段、分窗口、分屏幕等方式向个人信息主体展示左侧模板中的功能界面。	较 6 月 21 日版本版本基本无变化。
附录 C 交互式功能界面设计说明	2、 个人信息控制者需明确定义其产品（或服务）的核心业务功能，识别其必需收集的个人敏感信息。	2、个人信息控制者需明确定义其产品（或服务）的基本业务功能，识别其必需收集的个人信息。	较 6 月 21 日版本版本基本无变化。
附录 C 交互式功能界面设计说明	6、 附加业务功能是核心业务功能之外的其他功能，常见的附加业务功能如：提高产品（或服务）的使用体验的附加功能（如语音识别、图片识别、地理定位等）、提升产品（或服务）的安全机制的附加功能等（如收集密保邮箱、指纹等）。	6、扩展业务功能是基本业务功能之外的其他功能，常见的扩展业务功能如：基本业务功能基础上的一些衍生服务或新型业务、提高产品（或服务）的使用体验的附加功能（如语音识别、图片识别、地理定位等）、提升产品（或服务）的安全机制的扩展功能等（如收集密保邮箱、指纹等）。	较 6 月 21 日版本版本基本无变化。

	现行生效版本	6 月 21 日版本	10 月 22 日版本
附录 C 交互式功能界面设计说明	7、 附加业务功能一般具有可选择、可退订、不影响核心业务等特点，个人信息控制者在识别附加业务功能时需要充分分析其是否具备这些特点，不得将附加业务功能等同于核心业务功能，强制收集个人敏感信息。	7、扩展业务功能一般具有可选择、可退订、不影响基本业务等特点，个人信息控制者在识别扩展业务功能时需要充分分析其是否具备这些特点，不应将扩展业务功能等同于基本业务功能，强制收集个人信息。	7、 扩展业务功能一般具有可选择、可退订、不影响基本业务等特点，个人信息控制者在识别扩展业务功能时需要充分分析其是否具备这些特点，不应将扩展业务功能等同于基本业务功 能，强迫收集个人信息。
附录 D 隐私政策模板	XXXX 深知个人信息对您的重要性，并会尽全力保护您的个人信息安全可靠。我们致力于维持您对我们的信任，恪守以下原则，保护您的个人信息：权责一致原则、目的明确原则、选择同意原则、最少够用原则、确保安全原则、主体参与原则、公开透明原则等。同时，XXXX 承诺，我们将按业界成熟的安全标准，采取相应的安全保护措施来保护您的个人信息。	较现行生效版本基本无变化。	XXXX 深知个人信息对您的重要性，并会尽全力保护您的个人信息安全可靠。我们致力于维持您对我们的信任，恪守以下原则，保护您的个人信息：权责一致原则、目的明确原则、选择同意原则、最小必要原则、确保安全原则、主体参与原则、公开透明原则等。同时，XXXX 承诺，我们将按业界成熟的安全标准，采取相应的安全保护措施来保护您的个人信息。
附录 D 隐私政策模板	一、我们如何收集和使用您的个人信息 个人信息是指以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	业务功能一的个人信息收集使用规则	较 6 月 21 日版本版本基本无变化。

	现行生效版本	6 月 21 日版本	10 月 22 日版本
	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。 XXXX 仅会出于本政策所述的以下目的，收集和使用您的个人信息： （一） 为您提供网上购物服务【注：示例】 1、 业务功能一：注册成为用户。 为完成创建账号，您需提供以下信息：您的姓名、电子邮箱地址、创建的用户名和密码、……。 在注册过程中，如果您提供以下额外信息，将有助于我们给您提供更好的服务和体验：手机号、工作职位、公司、教育背景、……。但如果您不提供这些信息，将不会影响使用本服务的基本功能。 您提供的上述信息，将在您使用本服务期间持续授权我们使用。在您注销账号时，我们将停止使用并删除上述信息。 上述信息将存储于中华人民共和国境内。如需跨境传输，我们将会单独征得您的授权同意。	1、我们收集哪些您的个人信息 我们提供的业务功能需要依赖部分信息才得以运行。您选择使用该项业务功能，则需要向我们提供或允许我们收集的必要信息包括：…… 共计 XX 类个人信息。 您可自主选择向我们提供或允许我们收集下列信息：…… 共计 XX 类个人信息。这些信息并非该业务功能运行所必需，但这些信息对改善服务质量、研发新产品或服务等有非常重要的意义。我们不会强制要求您提供这些信息，您如拒绝不会对使用该业务功能产生不利影响。 在您使用该业务功能时，我们的 APP 会向您申请下列与个人信息相关的系统权限：…… 共计 XX 项系统权限。如果您不授权，将会导致我们无法提供该业务功能。除上述权限之外，您可自	

	现行生效版本	6 月 21 日版本	10 月 22 日版本
	2、 业务功能二：商品展示、个性化推荐、发送促销营销信息。 （略） 3、 业务功能三：与卖家沟通交流。 （略） 4、 业务功能四：支付结算。 （略） （二） 交付产品或服务【注：示例】 （略） （三） 开展内部审计、数据分析和研究，改善我们的产品或服务【注：示例】 （略） （四） …… …… 当我们要将信息用于本政策未载明的其它用途时，会事先征求您的同意。 当我们要将基于特定目的收集而来的信息用于其他目的时，会事先征求您的同意。	主选择是否额外授予 APP 其他的系统权限。 2、我们如何使用您的个人信息 对于必要的个人信息，我们会用来提供该项业务功能，包括……我们也会使用上述信息来维护和改进本项业务功能，开发新的业务功能等。 对于非必要的个人信息，我们会用于以下用途，包括……	

	现行生效版本	6 月 21 日版本	10 月 22 日版本
附录 D 隐私政策模板	我们如何使用 Cookie 和同类技术 （一） Cookie 为确保网站正常运转，我们会在您的计算机或移动设备上存储名为 Cookie 的小数据文件。Cookie 通常包含标识符、站点名称以及一些号码和字符。借助于 Cookie，网站能够存储您的偏好或购物篮内的商品等数据。 我们不会将 Cookie 用于本政策所述目的之外的任何用途。您可根据自己的偏好管理或删除 Cookie。有关详情，请参见 AboutCookies.org。您可以清除计算机上保存的所有 Cookie，大部分网络浏览器都设有阻止 Cookie 的功能。但如果您这么做，则需要在每一次访问我们的网站时亲自更改用户设置。如需详细了解如何更改浏览器设置，请访问以下链接： <Internet Explorer>、<Google Chrome>、<Mozilla Firefox>、<Safari> 和 <Opera>。	/	/

	现行生效版本	6 月 21 日版本	10 月 22 日版本
	（二） 网站信标和像素标签 除 Cookie 外，我们还会在网站上使用网站信标和像素标签等其他同类技术。例如，我们向您发送的电子邮件可能含有链接至我们网站内容的点击 URL。如果您点击该链接，我们则会跟踪此次点击，帮助我们了解您的产品或服务偏好并改善客户服务。网站信标通常是一种嵌入到网站或电子邮件中的透明图像。借助于电子邮件中的像素标签，我们能够获知电子邮件是否被打开。如果您不希望自己的活动以这种方式被追踪，则可以随时从我们的寄信名单中退订。 （三） Do Not Track（请勿追踪） 很多网络浏览器均设有 Do Not Track 功能，该功能可向网站发布 Do Not Track 请求。目前，主要互联网标准组织尚未设立相关政策来规定网站应如何应对此类请求。但如果您的浏览器启用了 Do Not Track，那么我们的所有网站都会尊重您的选择。		

	现行生效版本	6 月 21 日版本	10 月 22 日版本
	（四） …… ……		
附录 D 隐私政策模板	三、我们如何共享、转让、公开披露您的个人信息 （一） 共享 我们不会与 XXXX 以外的任何公司、组织和个人分享您的个人信息，但以下情况除外： 1、 在获取明确同意的情况下共享：获得您的明确同意后，我们会与其他方共享您的个人信息。 2、 我们可能会根据法律法规规定，或按政府主管部门的强制性要求，对外共享您的个人信息。 3、 与我们的附属公司共享：您的个人信息可能会与 XXXX 的附属公司共享。我们只会共享必要的个人信息，且受本隐私政策中所声明目的的约束。附属公司如要改变个人信息的处理目的，将再次征求您的授权同意。 我们的附属公司包括：……。	3、我们如何委托处理、共享、转让、公开披露您的个人信息 （1）委托处理 本业务功能中某些具体的模块或功能由外部供应商提供。例如我们会聘请服务提供商来协助我们提供客户支持。 对我们委托处理个人信息的公司、组织和个人，我们会与其签署严格的保密协定，要求他们按照我们的要求、本隐私政策以及其他任何相关的保密和安全措施来处理个人信息。 （2）共享 我们不会与本公司以外的任何公司、组织和个人分享您的个人信息，除非获得您的明确同意。目前，我们会在以下情形中，向您征求您对共享个人信息的授权同意：	较 6 月 21 日版本版本基本无变化。

	现行生效版本	6 月 21 日版本	10 月 22 日版本
	4、 与授权合作伙伴共享：仅为实现本政策中声明的目的，我们的某些服务将由授权合作伙伴提供。我们可能会与合作伙伴共享您的某些个人信息，以提供更好的客户服务和用户体验。例如，在您上网购买我们的产品时，我们必须与物流服务提供商共享您的个人信息才能安排送货，或者安排合作伙伴提供服务。我们仅会出于合法、正当、必要、特定、明确的目的共享您的个人信息，并且只会共享提供服务所必要的个人信息。我们的合作伙伴无权将共享的个人信息用于任何其他用途。目前，我们的授权合作伙伴包括以下 X 大类型： 1） 广告、分析服务类的授权合作伙伴。除非得到您的许可，否则我们不会将您的个人身份信息（指可以识别您身份的信息，例如姓名或电子邮箱，通过这些信息可以联系到您或识别您的身份）与提供广告、分析服务的合作伙伴分享。我们会向这些合作伙伴提供有关其广告覆盖面和有效性的信息，而不会提供您的个人身份信息，或者我们将这些信息	a) …… 了解此情形中目前涉及的公司、组织和个人，请点击此处。【提供超链接】 b) …… 了解此情形中目前涉及的公司、组织和个人，请点击此处。【提供超链接】 c) …… 了解此情形中目前涉及的公司、组织和个人，请点击此处。【提供超链接】 我们可能会根据法律法规规定，或按政府主管部门的强制性要求，对外共享您的个人信息。	

	现行生效版本	6 月 21 日版本	10 月 22 日版本
	进行汇总，以便它不会识别您个人。例如，只有在广告主同意遵守我们的广告发布准则后，我们才可能会告诉广告主他们广告的效果如何，或者有多少人看了他们广告或在看到广告后安装了应用，或者向这些合作伙伴提供不能识别个人身份的人口统计信息（例如“位于北京的 25 岁男性，喜欢软件开发”），帮助他们了解其受众或顾客。 2） 供应商、服务提供商和其他合作伙伴。我们将信息发送给在全球范围内支持我们业务的供应商、服务提供商和其他合作伙伴，这些支持包括提供技术基础设施服务、分析我们服务的使用方式、衡量广告和服务的有效性、提供客户服务、支付便利或进行学术研究和调查。 3） …… 对我们与之共享个人信息的公司、组织和个人，我们会与其签署严格的保密协定，要求他们按照我们的说明、本隐私政策以及其他任何相关的保密和安全措施来处理个人信息。		

	现行生效版本	6 月 21 日版本	10 月 22 日版本
附录 D 隐私政策模板	四、我们如何保护您的个人信息 （一） 我们已使用符合业界标准的安全防护措施保护您提供的个人信息，防止数据遭到未经授权访问、公开披露、使用、修改、损坏或丢失。我们会采取一切合理可行的措施，保护您的个人信息。例如，在您的浏览器与“服务”之间交换数据（如信用卡信息）时受 SSL 加密保护；我们同时对 XXXX 网站提供 https 安全浏览方式；我们会使用加密技术确保数据的保密性；我们会使用受信赖的保护机制防止数据遭到恶意攻击；我们会部署访问控制机制，确保只有授权人员才可访问个人信息；以及我们会举办安全和隐私保护培训课程，加强员工对于保护个人信息重要性的认识。 （二） 我们已经取得了以下认证：……。 （三） 我们的数据安全能力：……。 （四） 我们会采取一切合理可行的措施，确保未收集无关的个人信息。我们只会在达成本政策所述	我们如何保护您的个人信息 （一）我们已使用符合业界标准的安全防护措施保护您提供的个人信息，防止数据遭到未经授权访问、公开披露、使用、修改、损坏或丢失。我们会采取一切合理可行的措施，保护您的个人信息。例如，…… （二）我们已经取得了以下认证：…… （三）我们的数据安全能力：…… （四）我们会采取一切合理可行的措施，确保未收集无关的个人信息。我们只会在达成本政策所述目的所需的期限内保留您的个人信息，除非需要延长保留期或受到法律的允许。 （五）我们将定期更新并公开安全风险、个人信息安全影响评估等报告的有关内容。您可通过以下方式获得…… （六）互联网环境并非百分之百安全，我们将尽力确保或担保您发送给我们的任何信息的安全性。如果我们的物理、技术、或	较 6 月 21 日版本版本基本无变化。

	现行生效版本	6 月 21 日版本	10 月 22 日版本
	目的所需的期限内保留您的个人信息，除非需要延长保留期或受到法律的允许。 （五） 互联网并非绝对安全的环境，而且电子邮件、即时通讯、及与其他 XXXX 用户的交流方式并未加密，我们强烈建议您不要通过此类方式发送个人信息。请使用复杂密码，协助我们保证您的账号安全。 （六） 我们将定期更新并公开安全风险、个人信息安全影响评估等报告的有关内容。您可通过以下方式获得……。 （七） 互联网环境并非百分之百安全，我们将尽力确保或担保您发送给我们的任何信息的安全性。如果我们的物理、技术、或管理防护设施遭到破坏，导致信息被非授权访问、公开披露、篡改、或毁坏，导致您的合法权益受损，我们将承担相应的法律责任。 （八） 在不幸发生个人信息安全事件后，我们将按照法律法规的要求，及时向您告知：安全事件的基本情况和可能的影响、	管理防护设施遭到破坏，导致信息被非授权访问、公开披露、篡改、或毁坏，导致您的合法权益受损，我们将承担相应的法律责任。 （七）在不幸发生个人信息安全事件后，我们将按照法律法规的要求，及时向您告知：安全事件的基本情况和可能的影响、我们已采取或将要采取的处置措施、您可自主防范和降低风险的建议、对您的补救措施等。我们将及时将事件相关情况以邮件、信函、电话、推送通知等方式告知您，难以逐一告知个人信息主体时，我们会采取合理、有效的方式发布公告。 同时，我们还将按照监管部门要求，主动上报个人信息安全事件的处置情况。	

	现行生效版本	6 月 21 日版本	10 月 22 日版本
	我们已采取或将要采取的处置措施、您可自主防范和降低风险的建议、对您的补救措施等。我们将及时将事件相关情况以邮件、信函、电话、推送通知等方式告知您，难以逐一告知个人信息主体时，我们会采取合理、有效的方式发布公告。 同时，我们还将按照监管部门要求，主动上报个人信息安全事件的处置情况。		
附录 D 隐私政策模板	（一）访问您的个人信息 您有权访问您的个人信息，法律法规规定的例外情况除外。如果您想行使数据访问权，可以通过以下方式自行访问： 账户信息——如果您希望访问或编辑您的账户中的个人资料信息和支付信息、更改您的密码、添加安全信息或关闭您的账户等，您可以通过访问 XXXX 执行此类操作。 搜索信息——您可以在 XXXX 中访问或清除您的搜索历史记录、查看和修改兴趣以及管理其他数据。	（一）访问您的个人信息 您有权访问您的个人信息，法律法规规定的例外情况除外。如果您想行使数据访问权，可以通过以下方式自行访问：…… 如果您无法通过上述链接访问这些个人信息，您可以随时使用我们的 Web 表单联系，或发送电子邮件至…… 我们将在 30 天内回复您的访问请求。 对于您在使用我们的产品或服务过程中产生的其他个人信息，只要我们不需要过多投入，我们会向您提供。如果您想行使数据	较 6 月 21 日版本版本基本无变化。

	现行生效版本	6 月 21 日版本	10 月 22 日版本
	…… 如果您无法通过上述链接访问这些个人信息，您可以随时使用我们的 Web 表单联系，或发送电子邮件至 XXXX。我们将在 30 天内回复您的访问请求。 对于您在使用我们的产品或服务过程中产生的其他个人信息，只要我们不需要过多投入，我们会向您提供。如果您想行使数据访问权，请发送电子邮件至 XXXX。	访问权，请发送电子邮件至……	
附录 D 隐私政策模板	在以下情形中，按照法律法规要求，我们将无法响应您的请求： 1、 与国家安全、国防安全直接相关的； 2、 与公共安全、公共卫生、重大公共利益直接相关的； 3、 与犯罪侦查、起诉、审判和判决执行等直接相关的； 4、 有充分证据表明您存在主观恶意或滥用权利的；	在以下情形中，我们将无法响应您的请求： 1、与个人信息控制者履行法律法规规定的义务相关的； 2、与国家安全、国防安全直接相关的； 3、与公共安全、公共卫生、重大公共利益直接相关的； 4、与犯罪侦查、起诉、审判和执行判决等直接相关的； 5、个人信息控制者有充分证据表明个人信息主体	在以下情形中，我们将无法响应您的请求： 1、 与个人信息控制者履行法律法规规定的义务相关的； 2、 与国家安全、国防安全直接相关的； 3、 与公共安全、公共卫生、重大公共利益直接相关的； 4、 与刑事侦查、起诉、审判和执行判决等直接相关的； 5、 个人信息控制者有充分证据表明个人信息

	现行生效版本	6 月 21 日版本	10 月 22 日版本
	5、 响应您的请求将导致您或其他个人、组织的合法权益受到严重损害的。 6、 涉及商业秘密的。	存在主观恶意或滥用权利的； 6、出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人同意的； 7、响应个人信息主体的请求将导致个人信息主体或其他个人、组织的合法权益受到严重损害的； 8、涉及商业秘密的。	主体存在主观恶意或滥用权利的； 6、 出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人同意的； 7、 响应个人信息主体的请求将导致个人信息主体或其他个人、组织的合法权益受到严重损害的； 8、 涉及商业秘密的。
附录 D 编写要求	1、 详细列举收集和使用个人信息的目的，不得使用概括性语言。 2、 根据目的对应的不同业务功能，详细列出收集的个人信息类型。	1、详细列举收集和使用个人信息的业务功能，不应使用概括性语言。 2、根据不同业务功能，分别列出各业务功能所收集的个人信息类型。	较 6 月 21 日版本版本基本无变化。
附录 D 编写要求	7、 使用个人信息时，是否形成直接用户画像及其用途需要明确说明。	/	/
附录 D 编写要求	1、 如果个人信息控制者或其授权第三方使用自动数据收集工具收集个人信息，则需要对使用的技术机制做详细描述。 2、 常见的自动数据收集工具有：Cookie、脚本、Web 信标、Flash	/	/

	现行生效版本	6 月 21 日版本	10 月 22 日版本
	Cookie、内嵌 Web 链接、本地存储器等。 …… 4、 平台服务相关责任说明。如果个人信息控制者提供的服务属于平台服务（如：电商、社交、信息发布等），需要明确提醒用户其在上传、交流、发布共享个人信息时所面临的风险，并说明共享此类信息采取的安全措施。 …… 2、 可根据 GB/T AAAAA《信息安全技术 大数据服务安全能力要求》、 GB/T BBBBB《信息安全技术 数据安全能力成熟度模型》等国家标准确定自己的数据安全能力。 …… 4、 可重点提醒公众如何在使用产品或服务时保护好个人信息。		
附录 D 编写要求	/	/	新增： 如果产品或服务主要面向儿童，如有必要，隐私政策可以单独成章，或者单独成文，并突出

	现行生效版本	6 月 21 日版本	10 月 22 日版本
			征得监护人同意或监护人权利的条款。

5. 《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》最新版征求意见稿 与 0805 版本的比照

全国《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（草案）》于 2019 年 8 月公开向社会征求意见，得到密切关注。10 月 24 日编制组发布更新版草案。

我们详细比对了《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 8.5 版）》与《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 版）》，以表格的方式列出了两个版本中相应条款存在的主要区别，并以红色的字体标识。详细内容参见下表：[28]

	8 月 5 日版	10 月 24 日版
文件名	《信息安全技术 移动互联网应用（App）收集个人信息基本规范》	《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》 将原文件中所有涉及互联网“应用”均改为“应用程序”。
规范性引用文件		新增： GB/T 35273 信息安全技术 个人信息安全规范
移动互联网应用程序的定义	移动互联网应用： 安装、运行在移动智能终端上的应用程序，简称 App。	移动互联网应用程序： 安装、运行在智能移动终端上的应用程序，简称 App。
最小必要信息的名称及定义	最少信息 least（minimum）information	最小必要信息 minimum necessary personal information

[28] 作者：孟洁律师团队，https://mp.weixin.qq.com/s/pNSF9yvQnUNRgRWVxZOiPg。

	8 月 5 日版	10 月 24 日版
	保障某一服务类型正常运行所必需的个人信息，包括与服务类型直接相关，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，以及法律法规等规范性文件要求必须收集的个人信息。	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。
最小必要权限范围的名称及定义	最小权限范围 least（minimum） permission range 保障某一服务类型正常运行所必需的最少系统权限。	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。
移动互联网应用程序运营者的定义	移动互联网应用运营者 mobile internet application operator 是指移动互联网应用的所有者、管理者。	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。
App 收集个人信息基本要求	4.1 管理要求 App 收集个人信息应满足以下管理要求： a） App 运营者应履行个人信息保护义务，采取必要安全措施，保障用户个人信息安全。 b）当用户同意 App 收集某服务类型的最少信息时，App 不得因用户拒绝提供最少信息之外的个人	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，采取必要措施，保障个人信息安全； 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；

	8 月 5 日版	10 月 24 日版
	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少信息。 c）App 不得收集与所提供的服务无关的个人信息。 d）对外共享、转让个人信息前，App 应事先征得用户明示同意。当用户不同意，则不得对外共享、转让用户个人信息。 e）App 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。 f）用户明确拒绝使用某服务类型后，App 不得频繁（如每 48 小时超过一次）征求用户同意使用该类型服务，并保证其他服务类型正常使用。 g）App 应对其使用的第三方代码、插件的个人信息收集行为负责。第三方代码、插件收集个人信息视同 App 收集，App 应防止第三方代码、插件收集无关的个人信息。注：如第三方代码、插件自行向用户明示其收集、使用个人信息的目的、方式、范围，并征得用户同意，则第三方代码、插件独立对	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）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。 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； 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； 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。 h)在 App 运营者使用第三方代码或插件满足其特定功能时，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

	8 月 5 日版	10 月 24 日版
	其个人信息收集行为承担责任。 4.2 技术要求 App 收集个人信息应满足以下技术要求： a）当收集的个人信息超出服务类型的最少信息时，超出部分的个人信息，App 应逐项征得用户明示同意。 b）当同一 App 有 2 种或 2 种以上服务类型时，App 应允许用户逐项开启和退出服务类型，开启或退出的方式应易于操作。 c）当用户退出某服务类型后，App 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。 d）当申请个人信息相关权限或要求用户输入个人信息时，App 应向用户同步明示申请权限或收集信息的目的。 e）App 应向用户提供实时查询已收集个人信息类型的功能；查询结果应以独立界面展示，且查询方式应易于操作。 f) 存在对外共享、转让个人信息的，App 应向用户提供查询数据接收方身份的功能；查询结果应以独	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； 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； 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。 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； 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 开设独立界面的方式展示，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。

	8 月 5 日版	10 月 24 日版
	立界面展示，且查询方式应易于操作。 g）在技术可行且不影响终端和服务正常的情况下，App 应优先在用户终端中存储、使用所收集的个人信息。 h）App 应以实现服务所必需的最低合理频率向后台服务器发送个人信息。	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。 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。
附录 A.4:博客论坛最小必要信息范围和使用要求		新增：在法律法规要求的个人信息类型中新增： 仅对使用信息发布功能的用户收集，包括操作时间、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、用户发布信息记录。使用要求为《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》。
附录 A.5:网络支付最小必要信息的范围和使用要求		新增：在法律法规要求的个人信息类型中新增： 身份基本信息，包括国籍、性别、职业、住址、联系方式，使用要求为《支付机构反洗钱和反恐怖融资管理办法》。
附录 A.7:网上购物的功能定义、最小必要信息的范围和使用要求	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、交付等功能。 实现服务所需个人信息中收货人信息的使用要求：仅用于网上购物收货时识	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。 实现服务所需个人信息中收货人信息的使用要求：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。

	8 月 5 日版	10 月 24 日版
	别收货人、送达货物和联系收货人。	
附录 A.10:餐饮外卖最小必要信息的使用要求	实现服务所需个人信息中联系人信息的使用要求： 仅用于商家和配送员与用户取得联系和配送员送餐，姓名可无需真实。	实现服务所需个人信息中联系人信息的使用要求： 仅用于商家和配送员与用户取得联系和配送员送餐，姓名无需保证真实。
附录 A.14:金融借贷最小必要信息的范围和使用要求		新增：在法律法规要求的个人信息类型中新增： 偿付能力、贷款用途，使用要求为《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》。 在实现服务所需个人信息中将“个人征信信息”改为”个人信用信息”。
附录 A.17:运动健身最小必要信息的范围和使用要求		新增：在实现服务所需的个人信息类型中新增： 基本健康资料，包括性别、年龄、身高、体重，使用要求为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。
附录 A.18:问诊挂号最小必要信息范围		新增：在实现服务所需的个人信息的“医患沟通信息”中新增“过往病史”。
附录 A.19:网页浏览器的功能定义	A.19 浏览器 为用户提供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。	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。
附录 B:服务类型最小必要权限范围	附 录 B （规范性附录）服务类型最小权限范围列表	附 录 B （资料性附录）服务类型最小必要权限范围列表

	8 月 5 日版	10 月 24 日版
	本附录针对 Android6.0 及以上的危险权限，给出了服务类型的最小权限范围。	本附录针对 Android 6.0 及以上的可收集个人信息的权限，给出了服务类型的最小必要权限参考范围。

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