NEWSLETTER 数据合规

2019 第十一期 /总第十一期

数据合规时事速递

北京市环球律师事务所

2019 年 11 月 15 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. 国家新闻出版署发布《关于防止未成年人沉迷网络游戏的通知》

10 月 25 日，为规范网络游戏服务，引导网络游戏企业切实把社会效益放在首位，有效遏制未成年人沉迷网络游戏、过度消费等行为，国家新闻出版署近日发出《关于防止未成年人沉迷网络游戏的通知》。

《通知》从实行网络游戏用户账号实名注册制度；严格控制未成年人使用网络游戏时段、时长；规范向未成年人提供付费服务；切实加强行业监管；探索实施适龄提示制度；积极引导家长、学校等社会各界力量履行未成年人监护守护责任，帮助未成年人树立正确的网络游戏消费观念和行为习惯等六个方面提出了关于防止未成年人沉迷网络游戏的工作事项和具体安排。

《通知》出台的背景和意义

《通知》针对未成年人沉迷网络游戏、过度消费等行为，拟通过集中解决突出问题基础上，强调严格落实企业主体责任，依法履行政府监管职责，推动社会各界协同治理、有效参与，形成政府、企业、社会共管共治。《通知》的制定和实施，对于加强和改进网络游戏管理，切实保护未成年人身心健康，营造风清气朗的网络空间，具有重要意义和切实作用。

《通知》的具体要求与主要考虑

《通知》共提出六方面举措：

一是实行网络游戏账号实名注册制度。目前，游戏用户实名注册方式包括手机号、微信号、身份信息等多种方式。但实际使用中，不少未成年人使用家长手机号、微信号注册游戏账号，导致针对未成年人的管理制度难以真正落地。为此，《通知》要求严格实名注册，所有网络游戏用户均需使用有效身份信息方可进行游戏账号注册。

二是严格控制未成年人使用网络游戏时段时长。规定每日 22 时到次日 8 时不得为未成年人提供游戏服务，法定节假日每日不得超过 3 小时，其他时间每日不得超过 1.5 小时。具体标准主要是从合理分配未成年人日常作息时间角度提出，除

去正常睡眠、学习、用餐及文体活动时间外，区分节假日和其他时间，对游戏时段时长予以限定。这一规定既是对网络游戏企业和平台的要求，也是对监护人履行未成年人监护义务的指导。

三是规范向未成年人提供付费服务，规定网络游戏企业不得为未满 8 周岁的用户提供游戏付费服务；同一网络游戏企业所提供的游戏付费服务，8 周岁以上未满 16 周岁的未成年人用户，单次充值金额不得超过 50 元人民币，每月充值金额累计不得超过 200 元人民币；16 周岁以上的未成年人用户，单次充值金额不得超过 100 元人民币，每月充值金额累计不得超过 400 元人民币。主要参考《民法》总则中对民事行为能力的区分，以及有关方面就家长对孩子使用网络游戏消费限额意愿进行的抽样调查，并适当考虑目前未成年人实际付费状况。

四是切实加强行业监管。要求对未落实本通知要求的网络游戏企业，各地出版管理部门应责令限期改正；情节严重的，依法依规予以处理，直至吊销相关许可。

五是探索实施适龄提示制度。随着网络游戏类型越来越多样化，在题材、内容、玩法等各方面都可能存在不适宜未成年人体验的问题。《通知》要求网络游戏企业从多维度综合衡量，探索对网络游戏予以适合不同年龄段用户的提示，帮助未成年人、家长和老师等更好区分网络游戏，引导未成年人更好使用网络游戏。需要特别说明的是，适龄提示并不等同于西方的分级制度，决不允许色情、血腥、暴力、赌博等有害内容存在于面向成年人的游戏中。

六是积极引导家长、学校等社会各界力量履行未成年人监护守护责任，帮助未成年人树立正确的网络游戏消费观念和行为习惯。没有监护人的有效监督约束和陪伴陪护，有关制度的落实必然会大打折扣。

如何抓好《通知》的贯彻落实？

《通知》印发后，关键要认真贯彻和严格执行，把各项规定落实到位，让防沉迷的要求落地见效。

一是做好宣传解读。国家新闻出版署将通过组织研讨、培训等形式，向各地新闻出版管理部门和相关企业做好阐释解读，组织各地各单位认真学习《通知》，准确把握相关内容和要求。

二是强化督查落实。各地各单位要统一认识，严格落实《通知》要求，切实建

立健全相关工作机制。《通知》明确规定各属地管理部门要认真履行属地监管职责，加强对贯彻执行情况的监督检查，并协调有关执法机构做好监管执法工作。对《通知》落实过程中出现的问题，各属地管理部门要及时发现和纠正，对落实情况要及时报告。

三是完善配套制度。防止未成年人沉迷网络游戏的工作是一项复杂的系统性工程，需要各方面共同努力、积极推进，不断研究完善相关做法。目前，相关方面正抓紧推动《未成年人保护法》、《未成年人网络保护条例》的立法与修订工作，将防止未成年人沉迷网络游戏的要求写入法律法规，为各项具体工作提供更加有力的支撑。

同时，国家新闻出版署正与公安部对接，牵头建设统一的身份识别系统，为游戏企业提供游戏用户身份识别服务，以准确验证未成年人身份信息。我们还将逐步完善和丰富身份识别系统的功能，实现跨平台使用网络游戏时间的数据互通，以掌握每一个未成年人跨平台使用游戏的总时间并予以约束。随着网络游戏载体形式和服务方式的不断发展变化，我们将继续探索创新制度设计，不断总结好经验好做法，让防沉迷工作取得更大成效，为广大青少年健康成长保驾护航。[1]

《关于防止未成年人沉迷网络游戏的通知》全文参见：

http://data.chinaxwcb.com/epaper2019/epaper/d7110/d1b/201911/102212.html

2. 中国人民银行拟出台《个人金融信息（数据）保护试行办法》

据报道，《个人金融信息（数据）保护试行办法》初稿，已经由央行向部分银行进行了下发，待征求意见结束后将正式对外发布。按照规定，“（金融机构）不得从非法从事个人征信业务活动的第三方获取个人金融信息。同时，金融机构不得以“概括授权”的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。”

据了解，待《办法》正式出台后，银行将根据相关要求，对提供业务数据的第三方机构进行摸排，对于不能保证数据来源合法的数据供应商，要停止合作。

[1] 新华社。

事实上，当前持有个人征信业务牌照的机构仅百行征信一家，也就是说，各类以大数据风控为名，行个人征信之实的第三方大数据公司，理论上来说其经营行为为无牌的“非法”状态。

有媒体评论认为，监管此举，是对大数据行业的一次全面清缴整顿，尤其是一些存在灰色地带的三方大数据公司，将遭遇“灭顶之灾”。

如今，整肃个人金融信息泄露、篡改和滥用等数据源头，到底层第三方支付、金融科技产品认证规则的发布等层面，我国的金融科技监管体系正在逐步完善。

除了监管加强了对个人金融信息的保护，10 月 16 日，市场监管总局、人民银行两部委发文，决定将支付技术产品认证扩展为金融科技产品认证，并确定了《金融科技产品认证目录（第一批）》（以下称：认证备案），纳入 11 类金融科技产品，包括客户端软件、安全芯片、安全载体、嵌入式应用软件、云计算平台等。对上述 11 类产品，两部委指出，金融科技产品认证的基本认证模式为：型式试验+获证后监督。[2]

3．司法部副部长：个人信息保护法立法工作正加快推进

10 月 20 日，第六届世界互联网大会举行网络空间数据法律保护论坛，论坛以“安全与发展：数据治理的法治化”为主题。司法部副部长赵大程在论坛上介绍，当前，个人信息保护法已列入十三届全国人大常委会立法规划，相关工作正在加快推进，数据法律保护体系将得到进一步的健全和完善。

赵大程指出，加快完善数据保护法律规则体系。数据治理法治化的关键是形成一整套完善的法律规则体系，当前数据保护规则在很多方面还需要进一步完善，在统筹发展与安全、有效保护个体数据与促进数据资源开发利用等方面，还面临着不少的问题和挑战。

赵大程指出，要完善数据资源确权、开放、流通、交易相关制度，完善数据产权保护制度，为数据产业创新和数字经济发展提供制度基础。要完善数据保护法律规则，加大对技术专利、数字版权、数字内容产品及个人隐私等方面的保护力度，规范个人信息的收集、处理等活动，为维护网络数据安全提供更有利的法治保障。

[2] 新浪财经。

3

4. 俄罗斯《主权网络法》11 月 1 日生效。

俄罗斯“主权网络法”于 11 月 1 日正式生效,该法的推出受到了科技公司和网络用户的密切关注。根据法案,俄罗斯国家信息科技、通讯及大众传媒监察机构,可关闭外部网络联系,创造“纯俄”网络。

据报道,俄罗斯政府此前表示,“主权网络法”实施的目的在于保护国家,预防外国势力干预,也能维续国家网络的能力。《俄罗斯报》表示,“主权网络法”不会影响网络用户,但会确保俄罗斯网络在遭受威胁时的沟通能力。

有批评者警告称,由于“主权网络法”要求所有网络提供者,安装俄罗斯国家信息科技、通讯及大众传媒监察机构的特殊软件,恐让俄罗斯政府更容易监测或关闭网络,阻挡政治敏感内容。[4]

[3] 21 世纪经济报。
[4] 法制日报。

二、监管动态

1．工信部开展 App 侵犯用户权益专项整治行动

11 月 4 日，工业和信息化部发布《关于开展 APP 侵害用户权益专项整治工作的通知》（以下简称“工信部整治工作通知”），即日起，就 APP 违规收集个人信息、过度索权、频繁骚扰用户等侵害用户权益问题，开展信息通信领域 APP 侵害用户权益专项整治行动。工业和信息化部信息通信管理局在召开的整治工作启动会上表示，开展 APP 专项整治，是贯彻以人民为中心的发展思想，聚焦解决群众反映强烈问题的积极作为；是对前期四部委开展 APP 违法违规收集使用个人信息专项治理行动成果的巩固和深化；是创新监管方式的有益尝试。

本次整治行动将面向 APP 服务提供者和 APP 分发服务提供者两类主体对象，重点整治违规收集用户个人信息、违规使用用户个人信息、不合理索取用户权限、为用户账号注销设置障碍等四个方面的 8 类突出问题。整治工作分为企业自查自纠、监督检查和结果处置三个阶段，时间为 2 个月。

对于此次工信部门“整治工作通知”提到的四个方面的 8 类突出问题，App 专项治理工作组对其内容进行梳理、对照，供企业自查自纠过程中参考：

“工信部整治工作通知”内容		**App 专项治理工作组公布相关技术规范和标准文本中可参考的主要对应内容**
四个方面	**8 类突出问题**	
违规收集用户个人信息方面	私自收集个人信息	“认定方法”第三节：1.3.9 等； “自评估指南”评估点 20.23 等； “GB/T 35273”5.4 节等； “收集基本规范”第 4 章 b）c）l）等。
	超范围收集个人信息	“认定方法”第四节：1.2.5.6 等； “自评估指南”评估点 25.26.27 等； “GB/T 35273”5.2 节等； “收集基本规范”第 4 章 d）e）i）等。
	私自共享给第三方	“认定方法”第五节：1.2 等；

违规使用用户个人信息方面		“自评估指南”评估点 22 等； “GB/T 35273”8.2、8.7 节等； “收集基本规范”第 4 章 h）等。
	强制用户使用定向推送功能	“认定方法”第三节：4 等； “GB/T 35273”7.5 节等。
不合理索取用户权限方面	不给权限不让用	“认定方法”第四节：3.4 等； “自评估指南”评估点 24.26 等； “GB/T 35273”5.3 节 a）b）e）等； “收集基本规范”第 4 章 d）j）等。
	频繁申请权限	“认定方法”第三节：8 等； “自评估指南”评估点 28 等； “GB/T 35273”5.3 节 d）等； “收集基本规范”第 4 章 g）等。
	过度索取权限	“认定方法”第四节：1.7 等； “自评估指南”评估点 27 等； “GB/T 35273”5.2 节等； “收集基本规范”第 4 章 d）e）等。
为用户账号注销设置障碍方面	账号注销难	“认定方法”第六节：1.2.3 等； “自评估指南”评估点 30 等； “GB/T 35273”7.12 节等。

个人信息保护管理工作不可能一蹴而就、一劳永逸，亟待建立科学、长效的监督机制，以有效化解风险，促进发展创新，建设良好生态，引导对个人信息的良性开发利用。同样，企业的个人信息保护合规工作也是不断优化调整的过程，面对商业利益和个人权益、产品研发创新和用户合理诉求之间，还需不断探索寻求更加透

明、友好、合理的解决方案。[5]

2. 银行与大数据公司合作引监管关注 违规“爬虫”遭围堵

据财新报道，10 月 22 日，北京金融局窗口指导摸排区内所有大数据公司是否存在违规爬虫业务，如果没有则要求公司做出承诺函，如果存在违规爬虫业务，要上报并尽快整改。

另外 21 世纪经济报道称，中国人民银行、中国银保监会已组成调查组，摸底大数据的使用边界和采集边界，将会涉及外包催收公司管理办法。首批排查和调研的机构包括一诺银华、万盛金融和平安普惠。

其中，一诺银华是上海的一家资产处置公司，曾在 2015 年 10 月高调挂牌新三板，在取得挂牌同意函、全国建设分公司后，却因政策限制悄然退市。如今，另外一家催收公司湖南永雄又欲赴美上市，结果如何记者无从得知。

相关监管文件集中爆发。有银行内部人士透露，银行已经收到了通知，称央行发文紧急调研要求银行填写是否与第三方数据公司开展合作。排查内容涉及数据采集、信用欺诈、信用评分、风控建模方面，央行要求上报第三方数据公司的名字、股东背景、是否涉及爬虫。[6]

3. 监管加码整治，互金 App 野蛮发展时代落幕

当前，金融行业移动 App 安全问题引发业内关注，有行业报告评测超 13 万个金融 App，但发现有 70.22%存在高危漏洞，其中互联网第三方支付和信托类 App 的高危漏洞问题较为突出，保险、投资理财等分类的 App 高危漏洞问题也相对严重。不过，针对 App 违规整治也在逐步加深，**11 月 4 日，工信部宣布启动 App 侵害用户权益专项整治工作，专项整治时间为即日起至 2019 年 12 月 20 日**。有业内人士称，多种迹象显示，互金类 App 已成为当前个人信息泄露的重灾区,但在监管加大打压力度下，互金类 App 野蛮发展时代或将落幕。

[5] App 治理工作组。
[6] 新浪财经。

超七成金融 App 存高危漏洞 数据易泄露

近年来，随着智能手机和移动互联网的快速发展，移动 App 已深入应用至大众生活。一方面，金融类机构通过移动 App 展业，用户在 App 上进行投融资、借贷、交易支付等活动愈加频繁，另一方面，移动 App 在给大众生活带来巨大便利的同时，相应安全隐患也随之而来。

据中国信息通信研究院近日的发布《2019 年金融行业移动 App 安全观测报告》，截 2019 年 9 月 11 日，中国信通院从 232 个安卓应用市场中收录了超 13 万款金融行业 App，观测发现，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，其中部分高危漏洞甚至存在导致 App 数据泄露的风险。从 App 分类角度来看，互联网第三方支付和信托类 App 的高危漏洞问题较为突出，保险、投资理财等分类的 App 高危漏洞问题也相对严重。

近年来，尽管我国针对金融类 App 出台了多项规定，但随着获客、运营、风险等成本的水涨船高，仍有多数金融借贷 App 在收集个人信息时并未遵循最少够用原则，存在违规收集使用借款人个人信息，强制或直接默认读取通信录等情况。部分平台、借款人、催收公司、媒体、流量方的‘暗箱操作’，滋生了互金行业壳公司及内外勾结骗贷问题、恶意逃废债、暴力催收、敲诈勒索及黑市交易等乱象，这些乱象行为并非法外之地，尽管惩治互金乱象已具备一定的法制建设基础，但法制的不完善及巨大的利益引诱，仍驱使部分参与方游走在违法边缘。

互金类 App 违法违规情况突出，一方面是自身利益驱使，最为常见的是通过收集个人信息，进行大数据处理，进而在手机上推送相关消息影响用户，虽然转化过程较为缓慢，不过获利可观；另一方面则是相关法规规范配套不完善，虽然目前个人信息保护不是法律空白领域，但法规数量明显不够，尤其是没有形成层级保护，刑法的保护固然强大，但并不是侵犯到个人信息的行为都适用刑法，相关的行政法规配套不完善，对于企业的惩罚力度不够也是原因之一。

超 40 余家互金企业被点名整改 违规收集个人信息成重灾区

值得关注的是，当前，对于涉金融类互金 App 违法违规问题，工信部、公安厅、App 专项治理工作组等多方已屡次亮剑。

据不完全统计，仅在今年下半年，已有超 40 余家互金企业因 App 违法违规被点名整改。具体情况为：7 月 8 日，工信部点名 18 家互联网企业存在未公示用户

个人信息收集使用规则、未告知查询更正信息的渠道、未提供账号注销服务等问题，其中互金 App 包括暴风金融、51 人品贷、融 360、麦芽贷、九秒贷、布丁小贷、水象分期等。

此外，7 月 11 日、16 日， App 专项治理工作组相继两次通报，共 70 款 App 违规收集个人信息。北京商报记者注意到，其中违规涉金融类互金 App 数量占比近三成，被点名的机构包括趣店、快贷、旺信、趣店旗下来分期、闪电借款、及贷、借花花贷款、省呗、小花钱包、小赢卡贷、宜人贷借款、同花顺等 20 余家。

而至 8 月、9 月，广东省公安厅也相继曝光 App 违规行为，包括小牛在线、急用钱借钱、白鲸信用贷款、嘉联支付旗下立刷 App、鑫汇宝贵金属、口袋贵金属等互金类 App 被点名；此外，9 月 15 日，国家计算机病毒中心发布移动 App 违法违规问题及治理举措。其中，涉金融类应用方面分期宝等数款下载量很高的应用均名列其中。

值得注意的是，针对违规企业 App 整治惩罚，监管仍在加码。**11 月 4 日，工信部宣布启动 App 侵害用户权益专项整治工作，从现在开始针对当前用户反映强烈的一些侵害用户权益问题开展为期两个月的整治工作。**

工信部称，将重点针对违规收集个人信息、违规使用个人信息、不合理索取用户权限、为用户注销账号设置障碍四个方面开展规范工作，对私自收集个人信息、超范围收集个人信息、私自共享给第三方用户信息、强制用户使用定向推送功能、不给权限不让用、频繁申请权限、过度索取权限、为用户账号注销设置障碍八类问题进行整治。

据了解，**本次整治主要面向 App 服务提供者和 App 分发服务提供者（应用商店），主要专项整治工作分企业自查自纠阶段（自通知印发之日起至 11 月 10 日），监督抽查阶段（2019 年 11 月 11 日至 11 月 30 日）和结果处置阶段（2019 年 12 月 1 日至 12 月 20 日）。工信部对存在问题的 App 将统一进行通报，具体措施包括责令整改、向社会公告、组织 App 下架、停止 App 接入服务，以及将受到行政处罚的**违规主体纳入电信业务经营不良名单或失信名单等。

企业整改进行时 需做好事前合规准备

从工信部专项整治时间要求来看，留给机构整改的时间已然不多。对于整改进展，北京商报相继采访了前述被点名的多数互金 App，部分平台回复称目前已按相关规定上线了新版本，还有平台则称将按监管要求按时整改。

整改期间，互金类机构应注意哪些问题？国家互联网金融安全技术专家委员会（以下简称”专委会“）指出，金融类 APP 在采集个人数据方面，应当注意数据获取的最小化、必要性原则，专委会目前正在考虑利用区块链技术研发个人数据安全共享平台，通过用户自主控制个人数据的授权使用，企业在用户授权下、部门监管下阳光使用个人数据，减少互金类 APP 重复采集、过度采集、多头存储个人数据的成本和风险，保护用户作为个人数据主体的合法权益，促进个人数据的合规流动。[7]

4. 杭州互联网法院区块链智能合约司法应用上线

10 月 24 日，杭州互联网法院举行首个区块链智能合约司法应用新闻发布会，正式上线区块链智能合约司法应用，旨在高效处理违约行为，推进诉源治理，再造网络空间诚信。

2018 年 9 月杭州互联网法院司法区块链正式上线后不断升级，截至 2019 年 10 月 22 日，存证总量突破 19.8 亿条。

杭州互联网法院区块链智能合约司法应用，通过打造网络行为“自愿签约—自动履行—履行不能智能立案—智能审判—智能执行”的全流程闭环，设计司法治理机制和纠纷兜底处置助推智能合约的执行效率，高效处理少数违约行为，减少人为因素干预和不可控因素干扰，构建互联网时代下新的契约签署及履行形态，真正实现了网络数据和网络行为的全流程记录、全链路可信、全节点见证、全方位协作。

作为司法区块链的“2.0 版”，智能合约是以数字形式定义能够自动执行合同条款的合约，实现了从生成智能合约、完成实人认证并签约、合同原文及智能合约上传至司法区块链、智能合约自动运行、合约无法执行后转入多元调解流程、纳入信用联合奖惩机制、立案、审判、执行的全流程智能化，形成了集嵌套部署、信用奖惩、多方协同、司法救济于一体的集合化功能体系。

以合同的履行为例，传统合同是由买家和卖家协商、签约的，它的履行依托当事人的个人信用，如果一方违约，另一方需花费大量时间和精力维权。而智能合约则把合同的条款编制成一套计算机代码，在交易各方签署后自动运行，合同各方所有的协商、签署、履行、纠纷等过程都将一字不漏且无法篡改地被记录在司法区块链。一旦当事人违约，将由调解机构介入进行纠纷多元化解程序，相关数据将进入

[7] 北京商报。

司法区块链存证，若调解不成则在诉讼阶段推送至互联网法院诉讼平台。

目前，区块链智能合约司法应用已在部分网络购物合同里试点，下一步将努力实现在互联网法院集中管辖的范围内部署应用。[8]

5. 多款电商平台 App 存在隐私不合规行为被通报

11 月 8 日消息，国家计算机病毒应急处理中心近期开展电商平台整治行动，发现多款电商平台 App 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。

这些违法、违规移动应用具体如下：

1、未经用户同意收集个人隐私信息，涉嫌隐私不合规。具体 App 如下：《楚楚街》(版本 3.34)、《毒》(版本 4.17.0)、《萌推》(版本 2.5.0)、《淘集集》(版本 2.29.0)、《折 800》(版本 4.66.0)。

2、未向用户明示申请的全部隐私权限，涉嫌隐私不合规。具体 App 如下：《贝贝》(版本 9.26.01)、《返利》(版本 7.9.2)、《微店》(版本 5.7.8)、《找靓机》(版本 7.5.01)、《转转》(版本 7.1.2)。

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，第一时间监控未知病毒的入侵活动。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。[9]

6. 《2019 健康医疗行业移动 App 安全观测报告》发布

为了进一步贯彻落实习近平总书记网络强国战略思想，促进健康医疗行业安

[8] 中国法院网。
[9] 新华社。

全发展，为健康医疗行业管理部门、医疗机构和信息安全厂商提供决策参考，日前，在中国卫生信息与健康医疗大数据学会卫生信息安全与新技术应用标准委员会（筹）的工作会议上，中国信息通信研究院（以下简称“中国信通院”）安全研究所发布并解读了《2019 健康医疗行业移动 App 安全观测报告》（以下简称“《报告》”）。

《报告》由中国信通院安全研究所、卫生信息安全与新技术应用专业委员会和中国医院协会信息管理专业委员会组建的报告团队共同撰写，详细展示了全国范围内涵盖互联网医疗类、医疗机构类、健康管理类等的 8350 款健康医疗行业 App 的网络安全观测和风险分析成果。[10]

《2019 健康医疗行业移动 App 安全观测报告》全文参见：

http://www.caict.ac.cn/kxyj/qwfb/ztbg/201911/P020191111388712615123.pdf

7. 《物联网安全标准化白皮书（2019 版）》发布

10 月 27 日上午，在全国信息安全标准化技术委员会 2019 年第二次工作组“会议周”上，《物联网安全标准化白皮书（2019 版）》正式发布。

白皮书由中国移动通信集团有限公司、中国电子技术标准化研究院等 12 家企事业单位共同编制，重点介绍了国内外的物联网发展现状、安全法规政策及标准化进展，分析了物联网安全所面临的威胁和挑战，给出了物联网安全标准化体系框架，规划了相关标准工作重点，提出了开展物联网安全标准化工作的建议。[11]

《物联网安全标准化白皮书（2019 版）》全文参见：

https://www.tc260.org.cn/upload/2019-10-29/1572340054453026854.pdf

[10] 中国信息通信研究院。
[11] 中国信息通信研究院。

三、相关案例

1. 利用“撞库”盗取同行商业秘密被罚 35 万

10 月 31 日，杭州互联网法院对一起不正当竞争纠纷案进行公开宣判，判定被告“中服网”经营者及管理者浙江 C 网络科技公司立即停止对原告“女装网”运营方及管理者杭州 A 科技有限公司和杭州 B 科技有限公司的侵权，并赔偿两原告经济损失共计 35 万元，承担消除影响的民事责任。起因是 2018 年，有用户向女装网反映其账号被盗，这一反常现象立即引起女装网的关注。经查看后台，发现在此前 6 年间，有 4 个 IP 地址持续地登录网站会员账户，查看经销商数据。

经过调查，涉案会员账户登录访问的 IP 地址均在浙江 C 网络科技公司，并且是在不同时间、使用不同的品牌会员账户进行登录、访问“女装网”经销商数据库，且登录时间大多为工作日的 9：00—17：30。原来“中服网”利用了撞库的方式，也就是通过客户在两个同类网站上有可能使用相同的账户密码这一漏洞，来获取“女装网”上的信息。

最终，法院审理后认为，浙江 C 网络科技公司的行为已经构成不正当竞争。浙江 C 网络科技公司以不正当的手段获取“女装网”经销商数据，在涉案两个网站提供服务同质化的情况下，直接导致杭州 A 科技公司、杭州 B 科技公司客户群的流失和商业合作机会的减少，攫取了不正当的财产性权益。[12]

“撞库”是指黑客通过收集互联网已泄露的帐号和密码信息,生成对应的字典表,尝试批量登录其他网站后,得到一系列可以登录的用户。很多用户在不同网站使用的是相同的账号密码,因此黑客可以通过获取用户在 A 网站的账户尝试登录 B 网站。

该案针对目前的数据库信息市场指出三个重点:第一,互联网网站能否基于自身经营所收集、整理的用户数据库信息主张权利。目前能够达成共识的是,数据就是一种财产,是一种利益,是可以被保护的。互联网网站可以在用户同意的情况下,基于自身经营活动,就收集并进行商业性使用或具有商业价值的用户数据库信息主张权益。第二,是否构成互联网不正当竞争行为需要综合考虑同行业竞争者、网络用户和社会公众的利益。第三,账号密码与身份认证信息高度相关,其产生的财产性权

[12] 杭州网。

益具备计算机信息系统数据的法律属性,相关权益应属平台。

该案的裁判也为数据库的获取提供了清晰的指引——即在获取相关数据库信息时,应遵循合法、正当、必要限度的原则,可以在一定程度上从实现积极效果的目的出发对数据库信息进行利用,但不能通过不正当手段实质性替代原数据库开发者的服务。[13]

2. “人脸识别第一案”敲响个人信息保护警钟

近日，因为不愿意使用人脸识别，浙江理工大学特聘副教授郭兵将杭州野生动物世界告上了法庭。今年 4 月，郭兵在杭州野生动物世界办理了一张持有者可以在年卡有效期内无限次入园游玩的双人年卡。但在 10 月 17 日，他收到一条来自该动物园的短信，通知其携带年卡到园区办理人脸识别技术升级业务，否则将无法正常入园。这是国内消费者起诉商家的“人脸识别第一案”。

人脸识别也称面部识别，是基于人的脸部特征信息进行身份识别的一种生物识别技术，其作为继指纹比对、虹膜扫描、语音识别等之后的便捷生物识别技术，身份识别既快速又精准，已逐渐被应用于支付验证、住宅安防、出行通关等现实生活的各个领域。可以说，近年来随着该技术被越来越广泛地运用，国内已进入了“刷脸时代”。

“人脸识别第一案”的关注焦点主要集中于这两个问题之上。一是人脸识别技术在商用过程中的消费者权益保护问题；二是该技术运用带来快捷、便利的同时也隐含个人信息泄露风险的“双刃剑效应”问题。

《消费者权益保护法》规定：经营者不得以格式条款、通知、声明、店堂告示等方式，作出排除或者限制消费者权利、减轻或者免除经营者责任、加重消费者责任等对消费者不公平、不合理的规定，不得利用格式条款并借助技术手段强制交易。而该案中，动物园在未经游客同意的情况下，以短信通知方式单方面将指纹识别强制变更为人脸识别，实际是以通知方式变更双方在合同订立时约定的年卡使用条件，这既是对消费者正当权益的无视，也是对合同法的不遵守，有侵权、违约之嫌。因此，商家须尊重用户的选择权，在升级系统的时候，要与用户沟通且征得用户同意，倘若用户不同意，应该寻求有利于用户的方式解决问题，而不是逼迫用户必须

[13] 正义网。

完成“人脸识别”。

此外，人脸识别在具体应用过程中，必然要采集并保存含有人脸的图像或视频流。但包括人脸在内的图片等个人生物识别信息具有唯一性与敏感性，属于应受法律严格保护的个人信息。这些信息一旦出现泄露或被非法提供、滥用等，将会给用户带来不可预估的人身和财产安全危害，不能不令人担忧。事实上，《消费者权益保护法》亦明确规定，经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。如果说公权力机构为了公共安全使用人脸识别技术，具有正当理由，但像一些消费场所的经营者，也打着方便消费者的名义强制消费者使用人脸识别技术，就值得商榷了。

如今，“人脸识别第一案”已经被法院正式受理，再次敲响个人信息保护的警钟，让公众认识到个人脸部特征隐私信息保护的重要性，其积极意义不容小觑。司法机构应以此为契机，对商家的个人隐私信息采集行为予以界定，厘清人脸识别技术应用的法律边界问题，明确可采集的应用场景、使用范围、保管责任、违规处罚标准等，以避免商家随意越界采集、使用。只有法律更给力，相关规范更完善，才更有利于筑牢公民个人信息安全防护墙。[14]

3. 湖南网警发布“净网 2019”专项行动行政执法案例

“净网 2019”专项行动开展以来，湖南省公安机关聚焦网络安全行政执法，牢固树立主动进攻、标本兼治、生态治理理念，重点针对非法入侵计算机信息系统、不履行网络安全保护义务、侵犯公民个人信息等违法乱象开展清理整治，不断规范网上秩序，净化网络空间。截至目前，全省依据《中华人民共和国网络安全法》等法律法规共办理行政案件 687 起，警告 541 人（次），行政拘留 115 人，停机整顿 13 家（次），关停下架违法违规网络应用 693 款。

湖南网警发布“净网 2019”专项行动网络安全行政执法十大类典型

（1）网络运营者不履行网络安全保护义务

长沙某科技有限公司不履行网络安全保护义务案

[14] 训论。

2019 年 7 月 2 日，长沙市公安局高新分局网安大队工作中发现长沙某科技有限公司网站被攻击入侵，主页被篡改存有大量涉黄信息和广告信息。经查，该网站未落实安全技术措施、未制定内部安全管理制度、未明确网络安全责任人。

高新网安大队依据《中华人民共和国网络安全法》第 21 条、第 59 条规定，对该公司及直接负责主管人员周某分别予以罚款 10000 元和 5000 元，并责令立即整改到位。

宁乡某医院不履行网络安全保护义务案

2019 年 6 月 27 日，长沙宁乡市公安局网安大队工作中发现宁乡某医院官网存在高危安全漏洞，未采取有效安全技术措施防范风险，落实网络安全宁乡网安大队依据《中华人民共和国网络安全法》第 21 条、第 59 条规定，对该医院责令改正，予以警告处罚。

（2）非法利用信息网络

肖某利非法利用信息网络案

2019 年 3 月 13 日，株洲醴陵市公安局网安大队工作中发现违法嫌疑人肖某利自 2018 年 11 月以来，利用 QQ 群发布高价收购驾照积分等违法信息，非法获利 1000 余元。

醴陵网安大队依据《中华人民共和国网络安全法》第 46 条、第 67 条规定，对肖某利予以行政拘留 3 日，关闭用于实施违法活动的 QQ 群。

宋某辉非法利用信息网络案

2019 年 7 月 10 日，湘西保靖县公安局接群众举报，某电站职工宋某辉在成员近 200 人的微信群内发布一条时长约 1 分钟的色情视频，造成恶劣社会影响。

保靖网安大队依据《计算机信息网络国际联网安全保护管理办法》第 5 条、第 20 条规定，对宋某辉予以警告、并处罚款 200 元。

（3）网络运营者、网络产品或者服务提供者不履行个人信息保护义务

湘乡某电工实业有限公司不履行公民个人信息保护义务案

湘潭湘乡市公安局接上级通报，湘乡某电工实业有限公司网站存在泄露员工个人信息情况。经调查，发现该网站页面直接显示 296 名员工的详细信息（姓名、身份证号、电话号码等信息），未履行员工个人信息保护义务。

7 月 26 日，湘乡网安大队依据《中华人民共和国网络安全法》第 42 条、第 64 条第 1 款对该公司予以行政警告。

（4）利用信息网络传播暴恐视频

张某华利用信息网络传播暴恐视频案

2019 年 8 月 6 日，永州市公安局零陵分局网安大队工作中发现张某华发送暴恐血腥视频给其微信好友，而后该视频被多人转发，造成恶劣社会影响。

零陵网安大队依据《中华人民共和国反恐怖主义法》第 80 条第 2 项规定，对张某华予以行政拘留 10 日，并处罚款 1500 元。

（5）非法进行国际联网

唐某棋使用非法定信道进行国际联网案

衡阳市公安局蒸湘分局接群众举报，某学校有人使用 VPN 软件翻墙。经调查，唐某棋在自己电脑安装 VPN 软件进行国际联网，并试图将该软件及技术传授给他人。

2019 年 3 月 28 日，蒸湘网安大队依据《中华人民共和国计算机信息网络国际联网管理暂行规定》第 6 条、第 14 条规定，对唐某棋责令停止联网，予以警告处罚。

常德某网络游戏公司违规发布翻墙软件案

2019 年 3 月 26 日，常德市公安局武陵分局网安大队工作中发现常德某网络游

戏公司官网提供名为“极光加速器”的 VPN 软件供用户下载。经核实，该软件具备通过非法定信道进行国际联网功能。

武陵网安大队依据《中华人民共和国计算机信息网络国际联网管理暂行规定》第 6 条、第 14 条规定，对该公司予以行政警告。

（6）网络运营者不履行网络信息安全管理义务

桂阳某网站不履行网络信息安全管理义务案

2019 年 7 月 11 日，郴州桂阳市公安局网安大队工作中发现桂阳某网站出现赌博 APP 下载链接。经调查，该网站未对用户上传的“惠创金服”和“惠创国际”的两个涉嫌赌博的 APP 进行内容审核。

桂阳网安大队依据《中华人民共和国网络安全法》第 47 条、第 68 条规定，对该网站运营者予以警告处罚，并责令立即整改。

娄底某新闻网站不履行网络信息安全管理义务案

2019 年 4 月 8 日，娄底市公安局娄星网安大队工作中发现某新闻网站的社区论坛版块存在 1000 余条招嫖信息。经现场调查，该网站未履行违法信息处置和上报义务。

娄星网安大队依据《中华人民共和国网络安全法》第 47 条、第 68 条规定，对该网站予以行政警告，并责令关闭社区论坛进行整改。

（7）不履行联网备案职责

怀化某网络有限公司不履行国际联网备案职责案

2019 年 4 月 24 日，怀化市公安局鹤城网安大队工作中发现某网络公司门户网站自开通之日起 15 个月未向公安机关备案。同时，该公司开展的 IDC 业务未按规定留存租赁、托管的用户真实身份信息。

鹤城网安大队依据《计算机信息网络国际联网安全保护管理办法》第 11 条、第 12 条、第 23 条规定，对该公司予以警告处罚。

（8）利用信息网络扰乱公共秩序

徐某国利用信息网络扰乱公共秩序案

益阳市公安局赫山分局接群众报警称，有人扬言要用炸药炸掉益阳市富兴酒店。经调查，违法嫌疑人徐某国将烟花伪装成炸药放在密码箱内，拍摄照片后用微信发给宋某杰，并扬言将用 10 公斤自制雷管炸药炸掉宋某杰经营的富兴酒店。徐某国对其扬言实施爆炸扰乱社会秩序的违法事实供认不讳。

1 月 25 日，赫山网安大队依据《中华人民共和国治安管理处罚法》第 25 条第 3 项对徐某国予以行政拘留 10 日。

吴某伦利用信息网络散布谣言案

7 月 31 日，常德澧县公安局网安大队工作中发现违法嫌疑人吴某伦通过微信朋友圈及抖音上散布非洲猪瘟谣言的视频信息，造成一定社会影响。

澧县网安大队依据《中华人民共和国治安管理处罚法》第 25 条第 1 项规定，对吴某伦予以行政拘留 3 日。

向某利用信息网络扰乱公共秩序案

5 月 6 日，张家界慈利县公安局网安大队工作发现向某在新浪微博发布一段“法院警察打人了”不实视频，并配有“中国湖南省张家界市慈利县法院干警打老百姓，打伤打残多人”文字，造成大量网民对慈利司法机关产生误解，严重扰乱公共秩序。

慈利网安大队依据《中华人民共和国治安管理处罚法》第 25 条第 1 项规定，对向某予以行政拘留 10 日。

（9）非法侵入计算机信息系统

刘某明侵入计算机信息系统案

岳阳平江县公安局接群众报警称，所经营的网吧管理系统异常卡顿不能正常运行。经调查，违法嫌疑人刘某明在自己开设的网吧中，利用 DDOS、CC 等工具，攻击网上 APP 游戏、平江县其他网吧，构成了非法侵入计算机信息系统违法行为。

平江网安大队依据《治安管理处罚法》第 29 条第 1 项规定，对刘某明予以行政拘留 10 日。

（10）利用信息网络公然侮辱他人

安某利用信息网络公然侮辱他人案

7 月 19 日，邵阳市公安局大祥网安大队工作中发现违法嫌疑人安某在微信朋友圈公然发布侮辱交警言论。经查，安某在城南路段因洪水实行交通管制时期，对交警要求其到指定路段掉头心生不满，遂在网络上对交警进行辱骂，造成不良社会影响。

大祥网安大队依据《中华人民共和国治安管理处罚法》第 42 条第 2 项规定，对安某予以行政拘留 5 日。[15]

4. 明星信息贩卖背后：数据泄露来源难追踪，衍生代拍、刷关等产业

“能不能别帮我值机了，我机票都刷不出来了。”11 月 4 日晚上八点半，艺人李汶翰发布了这条微博，再次揭开艺人信息贩卖的黑幕一角。新京报记者调查发现，为躲避平台监管，从业者往往以身份证首字母缩写 sfz 代指。在其下游，还衍生出刷关、代拍、陪飞等多个产业。

“所谓刷关，就是根据爱豆航班信息，买同机次的票进了机场之后，匆匆见爱豆一面再把票退掉。”一位知情人士透露，“有些人想办站子（应援站），但自己没能力或者没时间去现场拍接机的照片，就会请代拍。”

[15] 中国西藏网。

泄露数据来源难追踪。“明星的信息泄露主要有以下几个方面：

第一，内部人员泄露。明星在入住酒店、搭乘飞机及参加活动时，航空公司、酒店、活动现场等工作人员很容易接触到明星的个人信息。有一些别有用心的人就把这些信息收集起来，进行出售。大部分明星的隐私都是在这种情况下泄露的，有的人为了逃避犯罪惩罚，专门开辟下级代理，本人只负责获取信息，并不直接出售。”

“第二，有些没有职业道德的狗仔队，专门挖掘调查明星隐私，甚至尾随跟拍。他们通过这种方式获取明星个人隐私后，将其高价出售，购买者再把这些信息提供给明星的粉丝。”

“第三，明星个人泄露。明星在参加各种活动及日常生活中，可能无意间说出自己的信息，或者在某些社交网站上发出个人信息。这种方式泄露的信息量较少，主要也是由其粉丝收集，影响不大。”

“第四，一些黑客及别有用心的不法分子，利用技术手段，窃取明星的各类账号，并由此挖掘其个人隐私并出售。”

案件侦破存技术难关。有接近警方的人士指出，侦破技术难度大系（此项产业泛滥的）关键原因。“报案人员认知不足，当隐私泄露事件发生到自己身上时，很少有人会去真的选择报警。加持发生于网络空间，证据固定存在一定难度。”

上述人士还表示，“再者，涉及数据的追踪和溯源，基层民警能力有限，缺乏技术支撑也是关键所在。在警力不足的情景下，很难分担大量警力和精力关注此类案件。”[16]

5. 李小璐 PGone 视频流出 用户隐私谁来保障

近日，PGone 职责某短视频网站流出其私密视频。PGone 的长文中提到，“为什么去年在某短视频网站拍的视频没有任何外传的前提下会被放出来没有 logo”。他在回应里说，视频是去年三四月录的，按照他的意思，应该是直接用 APP 录的，

[16] 经济日报。

但是这些视频他们没有外传过，这些视频是保存在他个人抖音的草稿箱里面。

（1）究竟是谁流出了保存在 PGoneAPP 私人草稿箱里的视频呢？

随后有网友爆料，指流出视频的源头是该 App 员工，从后台直接下载了人家草稿箱里的视频。

10 月 30 日深夜，针对 PGone 在微博指出的流出视频来自其该 App 草稿箱，App 官方回应称，该传言不实，草稿视频不会上传到运营审核后台，所以运营审核后台没有任何草稿视频，不存在 App 员工从后台下载草稿箱里传视频的可能，其他情况，App 还在继续核实。[17]

6. 争议学生注意力监控头环 创始人回应数据隐私与技术的质疑

近日，浙江金华的一所小学为了提高学习的专注程度，为学生们配置了一种被称为“脑机接口头环”的产品。根据公开信息显示，这款产品可以检测脑电波，评判学生上课、写作业时是否集中了注意力。同时，根据注意力集中的程度形成的分数，还会实时传输到老师的电脑上，也会像考试成绩排名一样被发到家长群里。

面对质疑，生产这款产品的 BrainCo（强脑科技）公司创始人韩璧丞 11 月 1 日在接受第一财经记者采访时对此事做出了回应，认为赋思训练系统，是用于做训练的产品，而不是用来监视的。

“它根本就没有监视的功能。”韩璧丞对记者表示，如果我有孩子的话，我是会很好地引导他来用产品做训练，我们很多员工的孩子，以及员工自己，都在使用公司的产品进行专注力训练，这样的训练和锻炼身体没有任何差别。

脑机接口并不是新鲜的科学技术，在业内简称为 BCI，通常是指通过在人脑神经与具有高生物相容性的外部设备间建立直接连接通路，实现神经系统和外部设备间信息交互与功能整合的技术。简单来说，就是实现用意念控制机器。它意味着，人与机器的主要交互方式，除了手工输入，以及近几年兴起的人工智能语音交互之外，还可以直接通过大脑向机器发指令。目前的脑机接口技术可以分为两类，一类是侵入式，比如在大脑中植入芯片，还有一类为非侵入式，比如戴上可以采集脑电

[17] 第一财经。

波的头盔或帽子。

（1）脑机接口技术距离全社会的普及还有一段距离

比如使用脑机接口设备的过程十分耗费脑力，选手需要注意力非常集中，才能让脑电波信号被脑机接口设备检测到，所以一段时间后大脑会感到很疲惫。

（2）另一个挑战则来自于数字伦理的挑战

随着 5G 时代即将到来，面向万物互联，人工智能的深度利用与广泛共享无法扭转。而在这样的时代，数字社会的技术伦理问题将会层出不穷。

今年 8 月，瑞典数据保护机构根据《通用数据保护条例》（GDPR）对当地一所高中开出罚单，原因是使用人脸识别系统记录学生的出勤率，这件事引发了教育机构中是否应使用人工智能技术的讨论。此外，欧盟在 2018 年出台的 GDPR 规定称，公司在收集用户包括面部等生物特征数据前必须经得个人同意，如有违反，企业可以被罚款金额达其全球收入的 4%。

今年 4 月 8 日，欧盟委员会发布人工智能伦理准则，以提升人们对人工智能产业的信任，列出了“可信赖人工智能”的 7 个关键条件——人的能动性和监督能力、安全性、隐私数据管理、透明度、包容性、社会福祉、问责机制，以确保人工智能足够安全可靠。欧盟将“人工智能”定义为“显示智能行为的系统”，它可以分析环境，并行使一定的自主权来执行任务。

根据官方解释，“可信赖的人工智能”有两个必要的组成部分：一是应尊重基本人权、规章制度、核心原则及价值观；二是应在技术上安全可靠，避免因技术不足而造成无意的伤害。

“我们充分保护学生隐私，赋思教育训练系统并没有将报告发给家长的功能，老师可以看到全班级的平均专注力，根据班级学生的专注力来调整教学方式。我们非常重视数据隐私的保护，BrainCo 的产品在使用过程中提取到的所有数据，都遵循欧盟 GDPR 商用资料的使用规范，上传到公司经过加密的云端数据库。”韩璧丞说。

他强调，在用户端，针对学校，老师，学生都有严格的数据方面的限制，公司

是没有办法超越自己角色的权限去查看数据的。[18]

7. 试行一天后，台铁人脸识别系统因“侵害隐私”停用

台“交通部”在台铁试运营人脸识别系统，结果在岛内引发巨大争议。6 日试行一天后，台铁宣布该系统停用。

据台湾中时电子报 6 日报道，2014 年 5 月 21 日台北发生的捷运随机杀人案震惊社会，“交通部”决定推动“智能监视系统示范计划”，“铁道局”最终在台铁丰原站耗资 2588 万元新台币试办。不过因该系统采用人脸识别功能，被认为侵害隐私。6 日，台铁决定拿掉人脸识别，只保留原本的动作侦测功能。

台湾一些地方已经使用人脸识别系统，像 7-11 便利店 2018 年在台北无人便利店导入人脸识别的进店离店和结算系统。今年 9 月，人脸识别解决方案又进入台湾某知名公立银行，并已全面用于该银行各营业网点的门禁和考勤管理系统。岛内法律界人士称，如果车站监控画面为公共场所，基本上没有侵害隐私权或个人信息，“但仍要看是否符合比例原则”。“消基会”交通组副召集人李克聪称，在车站使用人脸识别很两难，一方面担心侵犯隐私权，另一方面又想对通缉犯有预警机制。[19]

8. Uber 被责令进行为期 20 年的隐私审计，并被罚款 1.48 亿美元

根据法庭文件证实，Uber 曾使用比特币向持有敏感数据的黑客支付赎金。最终这两名男人被起诉电脑黑客和勒索罪名认罪，也使这一长期的法律诉讼落下帷幕，而优步和 LinkedIn 旗下培训网站 Lynda.com 付出了高昂的数据泄露代价。

黑客通过 Uber 和 Lynda.com 员工的 Amazon Web Services 登录来访问客户信息，从而入侵他们的服务器。然后，他们联系了这两家公司，勒索 uber 支付其比特币。

当时，uber 同意支付 10 万美元的加密货币。这笔款项是通过这家科技巨头的 HackerOne bug 赏金计划进行支付处理的，Uber 要求黑客签署一份保密协议，以防

[18] 第一财经。
[19] 环球网。

止他们使用数据并公开披露安全漏洞。

去年，来自加拿大的 VassieMergear 和 Florida 的 BrandonGlover 在从 Lynda.com 偷窃了 55000 个账户信息遭起诉，与 Uber 不同，Lynda.com 拒绝支付赎金。后来还发现两人是 2016 年入侵 Uber 肇事者，泄露 5700 万用户的数据。

优步将这一安全漏洞保密了一年多，直到 2017 年 11 月，其新领导层意识到这一点，决定将其公之于众。因此，Uber 被处以 1.48 亿美元的巨额罚款，并必须接受为期 20 年的隐私审计。Uber 还解雇了其首席安全官官 JoeSullivan，后者精心策划了向黑客付款的事宜，但是从未向公司用户发布有关安全漏洞的警备。

《纽约时报》，这两名定于明年被判刑的男子可能在联邦监狱中面临最高五年的最高刑期，并可能被处以最高 25 万美元的罚款。[20]

9. Facebook 再次发生数据泄露

全世界最大的社交网络公司 Facebook 之前因为不计其数的侵犯个人隐私的丑闻导致形象大跌，舆论要求扎克伯格引咎辞职。据外媒最新消息，Facebook 日前再一次发生了侵犯用户隐私权的事件，11 月 5 日，该公司披露称，多达 100 名第三方软件开发人员可能不当获取了用户隐私数据，包括社交网络上特定群组成员的姓名和个人资料、图片等。

最近发现，某些应用程序保留了对来自组 API 的组成员信息（例如与组活动有关的名称和个人资料图片）的访问权限，其访问时间超出了预期。

该公司承认安全漏洞，但 Facebook 拒绝提供有关应用程序开发人员，信息泄露程度以及受此数据泄露影响的用户数量的详细信息。该公司声称没有滥用的证据，但已通知开发人员立即删除保留的成员数据。Facebook 还计划进行审核，以确保已删除数据。尽管我们没有发现滥用的证据，但我们将要求他们删除他们可能保留的任何 Facebook 会员数据，并且我们将进行审核以确认该数据已被删除。尽管 Facebook 在 2018 年 4 月在其组 API 中进行了更改，但社交网络注意到一些应用程序仍在访问用户数据，从而发现了数据泄露。

[20] 洋洋说币。

谨在此提供信息，剑桥分析数据丢失丑闻之后， Facebook 检查了其软件开发框架并暂停了数千发现非法访问用户数据的应用程序。此外，与网上论坛集成的应用程序只能访问标准信息，包括网上论坛的名称，会员人数和网上论坛上发布的内容。

该公司吹嘘要成功限制开发人员对用户数据的访问，这一说法现已无效，因为 Facebook 本身已经承认某些应用程序仍在访问组成员的私人数据。该公司还指出，在过去 60 天内，大约有 11 个应用开发者非法访问了 Facebook 上的用户数据。

保护用户数据是 Facebook 一直努力征服的领域。臭名昭著的剑桥分析数据丢失丑闻和其他泄漏事件严重损害了其在全球用户中的形象。希望该公司该采取一些富有成效的步骤了，以确保用户数据不被泄露。[21]

在一系列丑闻发生后，Facebook 开始采取措施，限制第三方开发伙伴访问数据。另外，Facebook 也表示将开始进行转型，从 Facebook 传统上对外“广播”一切动态的社交模式转向移动聊天的私密社交模式，这意味着消费者公布的个人信息数量减少，面临的泄露风险也将减少。

该公司 9 月份表示，在剑桥分析丑闻之后，由于对其软件开发商生态系统的调查，它已经暂停了数万个第三方应用程序。[22]

10. Facebook Messenger 推出新隐私安全保护中心

Facebook 试图通过添加专用的集线器来提供使该 Messenger 用户更容易保护其对话免遭窥视的危险，该集线器提供有关隐私，安全性和安全性的信息。这本身不是功能更新，但是，如果您正在寻找使对话尽可能私密的方法，那么这是学习如何进行对话的最佳位置。

所谓的“隐私和安全中心”向 Messenger 用户显示了有关其隐私设置和诸如“秘密对话”之类的更多功能，这些功能可用于端到端的加密消息传递。随时随地都可以访问该网站，重点介绍了使用 Facebook 一段时间以来引入的工具的方式，包括阻止和报告，该工具应允许用户停止不必要的交互并报告诸如冒充名人朋友

[21] 超级盾云防御。
[22] 新浪财经。

的问题。

最重要的是，该中心包含有关 Messenger 用户如何通过登录警报和更安全的浏览以避免恶意软件来保护其帐户免受潜在黑客攻击的信息。此外，还提供有关 Facebook 如何删除虚假帐户并识别有害链接或图像以及减少错误信息传播的详细信息。

对于精通技术的人来说，Facebook 可以更深入地了解公司如何处理隐私和安全性，包括在幕后研究其中某些功能的工作原理。Facebook Messenger 用户可以访问网站的新部分 www.messenger.com/privacy，以获取有关隐私，安全性和安全性的所有详细信息。[23]

11. Apple Siri 和 Google Assistant 在隐私问题中暂停音频分级

谷歌和其他公司在智能扬声器和智能助手在场的情况下听到您尴尬的谈话或表情可能是一个开玩笑的笑话，但我们几乎不知道现实比小说还陌生。事实证明，出于改善服务的通常目的，陌生人实际上对其中一些(但不是全部)音频剪辑有所了解。但是，政府和监管机构将这一过程置于显微镜下，导致苹果和谷歌在欧洲试图评估隐私隐患并在可能的情况下围绕法律要求开展工作时暂停了此类系统。

苹果正式将其称为“分级”流程，但这是 Google 和 Amazon 共享的通用系统。毫不奇怪，这三个名称在有关如何使用和滥用该系统的不同公开中都已命名。简而言之，这些大技术公司向虚拟审核员(通常是承包商)发送了一个所谓的匿名音频片段，以评估和标记智能助手是否正确解释了音频。

现实情况是，这些音频片段实际上可能包含可能至少令人尴尬或在最坏的情况下可识别的信息。考虑到这些助手有时是偶然被触发的，这本身就是软件的缺陷，因此在用户不知情的情况下，很少有意外的东西被记录并发送给那些陌生人的可能性很小，要少得多。

据报道，谷歌和苹果都在对这些报告作出回应时搁置了他们审查程序的程序，并可能希望审查工作停止进行。CNBC 报道，谷歌已计划在欧洲停产三个月，而苹

[23] 虎财网。

果则在全球范围内暂停。

当然，这不是问题的永久终结。大技术公司不太可能停止采用这种方法，因为有时仍然需要人耳来验证 AI 的解释。苹果方面将使该计划成为自愿程序，并将首先询问用户，而不是假设他们已经同意了更一般的服务条款下的程序。报告中提到的另一家大技术公司亚马逊尚未采取类似行动。[24]

12．Google“南丁格尔计划”被爆秘密收集健康医疗数据 已涉及数百万美国人

2019 年 10 月 30 日，德国柏林数据保护机构（Berliner Beauftragte für Datenschutz und Informationsfreiheit，以下简称“柏林 DPA”）对德国上市房产公司 Deutsche Wohnen 因违反欧盟《通用数据保护条例》（General DataProtection Regulation，以下简称“GDPR”）做出了 1450 万欧元的罚款，是迄今为止德国数据保护机构对外做出的最高额罚款。

11 月 12 日消息，据国外媒体报道，谷歌与美国第二大医疗保健系统 Ascension 合作，通过名为“南丁格尔计划”(Project Nightingale)的项目收集和处理来自 21 个州的数百万美国人详细个人健康信息。

谷歌一直期望获取个人健康数据，并在医疗行业站稳脚跟，这似乎是其迄今为止开展的最大规模相关计划。亚马逊、苹果以及微软也在积极进军医疗保健领域，不过它们尚未实施如此大规模的项目。

去年谷歌秘密启动了“南丁格尔计划”，合作伙伴是 Ascension，它是由 2600 家医院、医生办公室和其他设施组成的连锁机构。内部文件显示，自去年夏天以来双方数据共享的步伐加快。

该计划涉及的数据包括检查结果、医生诊断和住院记录等类别，并形成完整的个人健康史，其中包括患者姓名和出生日期。

病人和医生都没有接到通知。据一位知情人士透露，至少有 150 名谷歌员工已

[24] 山东信息网。

经获得了大量患者的大部分数据。

据熟悉 Ascension 的人士透露，一些 Ascension 员工对数据收集和共享的方式提出了质疑。但隐私专家表示，1996 年通过的 HIPAA 法案一般允许医院在不告知患者的情况下与业务合作伙伴共享数据，前提是这些信息“仅用于帮助所涉及实体履行其医疗保健职能”。

在这种情况下，谷歌使用这些数据部分是为了设计新的软件，以先进的人工智能和机器学习为基础，针对患者护理提出建议。内部文件显示，谷歌母公司 Alphabet 员工可以接触到患者信息，其中包括研究科学部门公司 Google Brain 的部分员工。

谷歌云 Google Cloud 总裁 Tariq Shaukat 在发布会上表示，该公司的医疗保健目标集中在“改善结果，降低成本，拯救生命”。

Ascension 执行副总裁 Eduardo Conrado 说：“随着卫生保健环境继续迅速发展，我们必须进行变革，更好地满足我们所服务的人以及我们自己的护理人员和卫生保健提供者的需求和期望。”

谷歌和非营利组织 Ascension 有着类似的动机。到目前为止，谷歌已经指派了数十名工程师来为“南丁格尔计划”提供服务，但没有收取任何费用，因为它希望利用这个框架向其他卫生系统推销类似的产品。文档显示，谷歌的最终目标是创建一个综合性搜索工具，汇总不同的患者数据，并将它们整合在一起。

该项目由谷歌云部门负责。谷歌首席执行官桑达尔·皮查伊（Sundar Pichai）今年曾多次表示，为云计算寻找新的增长领域是当务之急。

Ascension 部分目标是改善对患者的护理。文件显示，该公司还希望挖掘数据以确定是否需要对患者进行额外检查。Ascension 还期望拥有一个比现有分散电子病历保存速度更快的系统。

谷歌成立之初的目标是组织全世界的信息，健康领域就一直是该公司高管们的兴趣所在。Google Health 是一项将现有医疗记录数字化的初步尝试，在经过三年的努力后于 2011 年被关闭。自那以来，Alphabet 已向旗下 Calico 和 Verily 等部门投入了数百万美元，这两个部门的目标分别是抗击衰老和控制疾病。

谷歌联合创始人拉里·佩奇(Larry Page)2014 年曾表示，担心自己医疗记录隐私

的患者过于谨慎。佩奇说：“我们并没有真正思考人们以正确方式与正确的人分享信息可能带来的巨大好处。”[25]

[25] 网易科技。

四、环球评论

1. 数据存储时间不符限制原则，房地产公司受德国 DPA 高额处罚

2019 年 10 月 30 日，德国柏林数据保护机构（Berliner Beauftragte für Datenschutz und Informationsfreiheit，以下简称“柏林 DPA”）对德国上市房产公司 Deutsche Wohnen 因违反欧盟《通用数据保护条例》（General DataProtection Regulation，以下简称“GDPR”）做出了 1450 万欧元的罚款，是迄今为止德国数据保护机构对外做出的最高额罚款。

一、案件背景及分析

Deutsche Wohnen 是一家房地产公司，被指使用没有删除功能的存储系统存储租户个人数据，进而导致数据的超期存储。被超期储存的数据包括租户的个人和财务状况信息，例如工资单、自我披露表、雇佣和培训合同摘要、税收数据、社保和健康保险数据以及银行对账单。2017 年 6 月，柏林 DPA 对该公司进行了现场调查后，即向该公司发出了违规警告。然而在 2019 年 3 月进行的另一次调查中，Deutsche Wohnen 仍无法解释为何没有清理租户个人数据或就超期储存租户存在任何法律依据。

柏林 DPA 认定，Deutsche Wohnen 超期存储不必要的、甚至是非法收集而得的个人数据的行为违反了 GDPR 第 25 条第（1）款以及 GDPR 第 5 条规定的处理的合法性原则。GDPR 第 25 条第（1）款规定，控制者在决定和实施数据处理的方法时，应当采取有效的、适当的技术、组织措施，例如数据匿名化和数据最小化，并且将必要的保障措施融入到处理之中以使数据处理既符合本条例的要求又能保护数据主体的权利。GDPR 第 5 条第（1）款规定，处理的个人数据应当是充足的、相关的、并且限于数据处理的最小必要范围（最小必要原则）；并且，以可识别数据主体身份形式存储的数据的存储时间不能长于实现个人数据处理目的所必须的时间（存储限制原则）。

二、行政罚款的计算

本案一大亮点为本案行政罚款的计算是柏林 DPA 首次依照德国数据保护机构 10 月 14 日公布的罚金计算模型来确定具体数额。

根据该模型，对企业的罚款金额是应按照以下五个步骤顺序进行分析确定：

1. 涉案企业的规模大小；

2. 企业平均年度营业额；

3. 每日平均罚款金额（即第 2 项平均年度营业额除以 360，如果企业年度营业额在 5 亿欧元以上，则最高限额为其年营业额的 2%-4%）；

4. 根据行为严重程度的不同，对于罚款乘以不同级别的因数（从 1-12 以上不等）；

5. 其他从重或从轻的因素。

本案中，首先考虑到 2018 年 Deutsche Wohnen 的年营业额超过十亿欧元（具体数额为 14.38 亿欧元），构成该模型中定义的大企业（第 VII 类，年度营业额超过 5 亿欧元）类别，该类别大企业的平均年度营业额为该企业的实际年度营业额，即 14.38 亿欧元。

其次，由于 Deutsche Wohnen 年度营业额在 5 亿欧元以上，则其罚款最高限额为其年营业额的 2%-4%。

再次，根据 GDPR 第 83 条（5）款（a）项的规定，对违反 GDPR 第 5 条规定的数据处理的基本原则（即合法、公平和透明原则；目的限制原则；最小必要原则、准确性原则；存储限制原则；完整性和保密性原则以及责任原则）的行为，可以处以该组织上一财政年度全球营业总额 4%的行政罚款；GDPR 第 83 条（4）款（a）规定，对违反 GDPR 第 25 条规定的数据控制者的义务的行为，可以处以该组织上一财政年度全球营业总额 2%的行政罚款。

值得注意的是，本案中，考虑到 GDPR 第 5 条对于个人数据处理基本原则一定程度上理解起来比较宽泛，柏林 DPA 并没有以年营业额 4%作为罚金的上限，而是更为谨慎地以年营业额 2%作为罚金的上限，即最高额 2800 万欧元对公司予以处罚。

最后，为了进一步确定具体的罚款金额，柏林 DPA 考虑了如下从重或从轻处

罚因素：

一方面，Deutsche Wohnen 采取的存储系统不能删除租户的个人信息，进而导致超期存储，侵犯租户对个人信息享有的权利以及违反了 GDPR 的相关规定，Deutsche Wohnen 对此主观上持有故意，放任这种情况的发生，情节较重；同时，公司采取了初步措施来纠正这种情况，并积极配合监管机构工作。综合上述因素，柏林 DPA 最终对 Deutsche Wohnen 做出了 1450 万欧元的罚款。

三、警惕数据坟墓（Datenfriedhöf）

柏林 DPA 负责人 Maja Smoltczyk 在报道中称，“非法大规模存储个人数据极为普遍。这种不当行为潜在危险极大，而且只有发生网络攻击等安全事故后我们才能发现它的存在。GDPR 的立法主旨是保护公民的个人数据免受非法处理或侵犯，我们希望所有的企业都能遵守 GDPR 的要求，合法地处理个人数据。”

该项行政处罚尚未终局。据悉，Deutsche Wohnen 已对柏林 DPA 的处罚提出异议，并将在柏林地方法院（Landgericht）上与柏林 DPA 对簿公堂。该公司指出，本案中柏林 DPA 指控的、不能删除租户个人数据的存储系统已经被更换，并再次强调公司没有以不被允许的方式向第三方披露租户的个人数据。我们将持续关注本案的后续进展。[26]

[26] 作者：孟洁律师团队，https://mp.weixin.qq.com/s/8uoh0L-FpGMKZ-h3WtNZxw。

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