

考拉征信被查： 谨防“爬虫”变“害虫”

即将出台的《个人信息（数据）保护试行办法》，侧重于完善征信机制体制建设，将对金融机构与第三方之间征信业务活动等进一步做出明确规定，加大对违规采集、使用个人征信信息的惩处力度。

文 | 夏木



11月20日，央视报道了7家涉嫌侵犯公民个人信息犯罪的公司。拉卡拉支付旗下的北京考拉征信服务有限公司赫然在列。其涉嫌非法提供身份证返照查询9800多万次，获利3800万元。11月20日当天，创业板上市公司拉卡拉股价午后跌停跳水，市值蒸发约20亿。

考拉征信并非草台班子，它曾是首批获央行备案开展企业征信和批准开展个人征信业务准备的八家机构之一，也是百行征信有限公司的发起方之一。但恰恰因为正规背景，所以更令人担忧——如果连“根正苗红”的征信公司都会越雷池，那么公众的个人隐私和网络信息安全更要打上问号。

从信用管理人到信息泄露者

考拉征信出了什么问题？这一切要从一起公民个人信息贩卖事件说起。

2018年4月，江苏淮安警方发现，有人在网非法购买公民个人信息。嫌疑人高某主动投案，他声称自己花500块钱从网名叫“过去、将来”的手里购买了317条公民个人信息。每条公民个人信息折合不到两元钱。信息包括手机号、姓名、身份证号和家庭地址。警方顺藤摸瓜，依次将这个链条上的申某，以及广州诺涵科技公司、湖南九象公司、北京黑格科技有限公司等相关人员抓获，最后从黑格科技追查到北京考拉征信服务有限公司。

这些公司除了购买公民个人信息，还和其他公司相互交换公民个人信息，并通过爬虫技术手段获取公民个人信息，用于公司放贷和非法出售牟利。而考拉征信是这些公司的上游环节之一，起到的核心作用就是提供“身份核验返照”，也就是输入公民姓名和身份证号码，就可以获取公民带网纹的二代身份证彩色照

片。利用这些身份证照片和公民个人信息，不但可以进行“精准营销”，将他们拉到非法信贷平台上，还可以在发生逾期后，轻而易举地进行催收。

有意思的是，这些持有公民个人信息的公司既做自营又做平台。警方发现，广州诺涵信息科技有限公司将公民个人信息称为“流量”进行买卖，同时公司也开发乐花管家等多个小贷平台，在自身购买公民个人信息用于推销贷款，软暴力催收的同时也和其他公司相互交换公民个人信息，还开发有爬虫软件，通过技术手段抓取其他小贷公司的公民个人信息，用于公司放贷和非法出售牟利。

据警方调查发现，诺涵科技的公民个人信息，主要来自湖南九象信息有限公司。这家公司开发了一个黑爬虫网站，通过爬虫软件非法获取数10家小贷公司的公民贷款和逾期数据，然后公开提供收费查询，并提供“身份核验返照”业务，任何人只要在该网站输入公民姓名和身份证号码，就可以查询获取公民身份证相片。经审讯，九象公司黑爬虫网站的“身份核验返照”业务端口来自北京黑格科技有限公司，而黑格科技的查询接口，则是从北京考拉征信服务有限公司等4家公司购买的。

考拉征信作为一家第三方信用评估及征信管理服务商，从上游公司获取接口后，又违规将查询接口出卖，并非法缓存公民个人身份信息，供下游公司查询牟利，从而造成公民身份信息包括身份证照片的大量泄露。2015年3月以来，北京考拉公司非法提供查询返照9800余万次，获利3800余万元，在公司服务器中查获并收缴被非法获取、存储的公民姓名、身份证号、照片近1亿条。

公民身份认证服务是直接服务于“互联网

考拉征信作为一家第三方信用评估及征信管理服务商，从上游公司获取接口后，又违规将查询接口出卖，并非法缓存公民个人身份信息，供下游公司查询牟利，从而造成公民身份信息包括身份证照片的大量泄露。

市场上鱼龙混杂，个人隐私保护法至今没有出台，信息买卖依然处于无监管地带。

+ 政务”来提升政府公共服务效能，达到防范欺诈和金融风险的目的。但是，涉案公司非法将公民身份认证端口出售，并非法缓存公民身份数据。身份证照片可以随意获取，这为小贷公司实施“套路贷”犯罪、暴力催收打开了罪恶之门。

黑色产业链浮出水面

调查发现，倒卖信息的贩子频繁发布贩卖广告，以 30 元的价格便能购买到 10 套文件，其中每套包括个人手持身份证照片，身份证正面、反面各一张。信息贩子声称，如果做网贷的话，这些身份证信息都是一手的“料”。

熟悉征信业务的业内人士透露，通常被泄露的身份证正反面照片大部分来源于金融贷款机构，注册 POS 机、注册 APP 账号时的信息也会被泄露。有的 APP 注册要上传照片，认证完以后，照片自然而然就会被这些公司保存。一般来讲，金融贷款公司和支付公司存有此类照片较多。多数是用户注册认证完以后，照片资料就会在这些公司数据库内，一旦监管不到位或者有内鬼，便会有隐私泄露的可能性。

倒卖信息的情况泛滥成灾。2019 年 7 月，广东省公安厅官网公布，在 2019 年第二季度超范围收集用户信息 APP 清理整治工作中，共监测发现 1048 款 APP 存在超范围收集用户信息行为。其中，酷狗音乐、艺龙旅行等 42 款 APP，存在超范围读取用户通话记录、短信或彩信，收集用户通讯录、用户设备上已知账号，超权限使用用户设备麦克风等突出安全问题。近期，工信部对外披露二季度检测发现问题的应用软件名单，多个在线直播平台如 YY、斗鱼直播，美团外卖、91 短贷等 32 款应用软件被点名，这些应用多涉未经用户同意，收集、使用用户个人信息。

市场上鱼龙混杂，个人隐私保护法至今没有出台，信息买卖依然处于无监管地带。高利贷、超利贷屡禁不绝，某种程度上和一些第三方大数据科技公司违规为其提供金融数据、风控服务等不无关系，一旦没有这些支持，高利贷、超利贷平台在反欺诈、风控业务运作上会面临非常大的考验。爬虫技术有利于挖掘数据价值，它本身是中性的，但部分第三方数据公司在与其他金融机构合作过程中，留存部分数据，又把这些数据转手倒卖给第三方消费信贷公司，甚至是现金贷、高炮台公司，使得用户数据被滥用，用户权益被严重侵犯。

公安部针对考拉征信案件暴露出的行业乱象，全面开展了打击整治工作。截至 2019 年 11 月底，警方共立案侦查侵犯公民个人信息案件 29 起，抓获犯罪嫌疑人 288 人，缴获公民个人信息 4.68 亿余条，涉案金额 9400 余万元。涉案公司非法缓存的公民身份认证数据现已全部收缴。同时，堵塞漏洞，“身份核验返照业务”接口全部封停，公安部门会同中国人民银行等部门，加强对公民身份认证服务、个人征信服务的监管。

监管迫在眉睫，外国经验或可参考

从法源上，对非法爬虫并非无法可依。

2017 年 6 月 1 日实施的《网络安全法》明确规定，任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具。

2019 年 5 月 28 日，国家互联网信息办公室就《数据安全管理办法（征求意见稿）》公开征求意见。对于网络运营者超出运营需要收集

个人信息的行为,《办法》作出了限制性规定,对“网络产品核心业务功能运行的个人信息”以外的信息,网络运营者不得因个人信息主体未同意收集而拒绝提供核心业务功能服务。

针对网络爬虫等抓取网页的自动化手段,《办法》明确应不妨碍网站正常运行,并列明具体的访问收集流量不得超过网站日均流量的1/3。针对手机APP过度获取权限的问题,要求“网络运营者不得以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由,以默认授权、功能捆绑等形式强迫、误导个人信息主体同意其收集个人信息”;对数据泄露才确定网络安全负责人的问题,其明确数据安全责任人的任职要求,突出网络运营者主要负责人、数据安全责任人的姓名及联系方式等。

更重要的是,《办法》还新增了两项配套的制度性规定,用以更好地落实政府部门对数据安全的监督。一是重要数据和个人敏感信息的备案,“如果网络运营者以经营为目的收集重要数据或个人敏感信息的,应向所在地网信部门进行备案。”二是数据安全认证和应用程序安全认证制度,“国家鼓励网络运营者自愿通过数据安全认证和应用程序安全认证,鼓励搜索引擎、应用商店等明确标识并优先推荐通过认证的应用程序。”

就个人数据保护的监管问题,我们或许还可以参照欧美经验。

欧洲是数字监管的严格先行者,2016年4月,欧盟通过《数据保护通用规则》(GDPR)草案,对用户画像技术的使用进行了限制。在大数据时代下,用户画像是非常普遍的技术使用和业务拓展行为,比如这个用户喜欢买什么,这个用户喜欢逛什么样类型的网站,可以利用用户画像技术获得。但GDPR对用户画像技术设置了一系列红线,比如不允许分析结果涉及

儿童,不允许分析结果导致对某些个人的歧视,不允许分析结果可能产生某种法律上的偏向性的建议等等。

2018年5月25日,GDPR正式生效,确立了比以往更加严格的个人数据处理的统一规范,增加了用户个人数据保护的权力,同时对企业收集和使用个人数据,提出了更高的透明度要求。其违规处罚力度也超过以往。每一单违规行为将受到高达2000万欧元或者上一年全球年营业额的4%的严重处罚,以两者中较高者为准。且只要企业数据处理活动涉及欧盟公民数据,都会受到该法规的限制。所有手机APP只要有欧盟公民使用就需要合规。

在美国,目前既没有专门的数据保护法律法规,也没有对应的职能部门对此进行监管。不过,在州一级层面,已经有案例显示美国正在效仿欧盟的GDPR:2018年6月29日,美国加利福尼亚签署了一项数据隐私法案,里面不少条款同《通用数据保护条例》中的核心条款相同。该法案将从2020年1月开始生效,并适用于加利福尼亚州用户(硅谷所在地)。该法案规定,对于掌握超过5万人信息的公司,用户有权查阅自己的哪些数据被收集,并要求公司删除自己的数据,以及拒绝将数据卖给第三方。单次违法将被处以7500美元的罚款。

在我国,值得注意的是即将出台的《个人金融信息(数据)保护试行办法》。这一办法侧重于完善征信机制体制建设,将对金融机构与第三方之间征信业务活动等进一步做出明确规定,加大对违规采集、使用个人征信信息的惩处力度。结合对于考拉等公司的重拳出击,对违规爬虫的整治力度日趋加大,一方面是对个人金融信息的保护意识不断加强,另一方面也是对于个人征信业务的规则不断明确的结果。E