据央视网报道，2019年底，江苏淮安警方依法打击了7家涉嫌侵犯公民个人信息犯罪的公司，涉嫌非法缓存公民个人信息1亿多条。

其中，拉卡拉支付旗下的考拉征信涉嫌非法提供身份证返照查询9800多万次，获利3800万元。

一条隐秘的身份信息非法核验链条随之浮上水面。

“身份信息核验返照”是指通过输入公民姓名和身份证号码查询获取身份证相片，属于身份信息核验的一种方式。

最早的身份信息核验服务由2001成立的全国公民身份证号码查询服务中心（NCIIC）提供，其利用公安部数据库比对后返回“一致”或“不一致”的结果。

2012年起，国家陆续出台相关法律法规，要求互联网用户遵循“后台实名、前台自愿”的原则，基于手机号等进行真实身份信息认证；支付机构则进一步被要求核对用户有效身份证件并留存复印件。

如今，无论是办理手机卡，住酒店，购买火车票还是注册App账号，要么需要输入手机号和短信验证码，要么需要输入姓名和身份证号。这些信息都是为了做身份信息核验，从而证实“你是你”。

随着实名认证的普及，公安部以外的其他政府部门、金融机构甚至互联网公司等也具备了大量收集公民身份信息的可能。
身份信息核验市场愈发庞杂，不再是一家独大的“生意”，逐渐衍生出灰色地带。

需求飞涨

最早开始提供身份信息核验服务的NCIIC成立于2001年。

人们在电信营业厅、银行等机构办理业务时，需要出示身份证件，随后姓名和身份证号等数据会被传送至公安部“全国人口信息社会应用平台”进行比对，返回“一致”或“不一致”的比对结果。

据官网介绍，该服务涵盖了政府部门及银行、保险、证券、汽车金融、消费金融、互联
网支付、
征信、电子商务、
通信、物流、人力资源等十余个行业

的用户。
但是据南都记者了解，真正获得查询接口的企业并不多——曾有业内人士估计，全国只有几十家。

中国银联“身份证信息认证和查询”业务负责人告诉南都记者，NCIIC原则上只提供给事业单位或各行业持牌机构，门槛极高，而且查询接口的运行时间仅为5*8小时，查询次数也有限制。

但不可忽视的是，身份信息核验市场规模飞速增长。

《2018年互联网和相关服务业经济运行情况》数据显示，游戏、社交等八类App下载量超过千亿次。

以游戏为例，根据《中国互联网络发展状况统计报告》，2018年的游戏用户为4.84亿。假设每个用户平均注册两种游戏，身份信息核验的次数将高达近10亿次/年。

据前瞻产业研究院发布的《中国身份认证信息安全行业与前景预测分析报告》统计，2018年，中国网络身份认证信息安全行业市场规模达到132亿元，到2022年将接近300亿元。

一边是不足百家拥有身份信息核验接口的企业，另一边是百亿量级的市场需求，巨大的缺口嗷嗷待哺。
近年来NCIIC的收费标准的变化或许也能佐证身份信息核验市场的供不应求。

2017年，发改委决定取消公民身份认证服务收费政府定价，具体收费标准由NCIIC与用户商定。

2019年7月，NCIIC宣布取消公民身份信息核验服务收费，并取消通过合作伙伴提供公民身份信息核验服务的模式。原通过合作伙伴使用公民身份信息认证服务的用户将由NCIIC提供免费认证服务。

也就是说，NCIIC未来只会向符合资质要求的用户直接提供免费的身份信息核验服务，不再下设代理商（即“合作伙伴”）间接提供服务。NCIIC还曾向媒体表示，取消收费后有很多机构在排队，接入时间无法确定。

然而，在过去十几年间，随着实名制的普及，新“玩家”不断涌现，最上游的查询接口提供商与下游企业
之间早已形成了庞杂的中间市场——
公安部不再一家独大，有能力合法留存大量公民身份信息的其他政府机构、运营商

、银行、大型互联网企业也纷纷加入“战局”。

“身份证号码、电话号码和和姓名，很多的机构都有”，一位曾在运营商工作的专家对南都记者说，比如12306、人力资源和社会保障部，还有医疗单位、婚姻登记处，“其实数据源特别多”。

此外，身份认证方式也从最基础的身份证二要素（姓名、身份证号）逐渐拓展到运营商三要素（姓名、身份证号、手机号）、银行卡三要素（姓名、身份证号、银行卡号）、银行卡四要素（姓名、身份证号、银行卡号、银行预留手机号），还可配合人脸识别使用。

多位数据接口服务商指出，最上游的身份信息核验接口通常来自公安系统、运营商和银联。

多级链条

以银联的身份证信息认证和查询业务为例。

银联开放平台官网介绍称，该产品可获得公安部直联实时数据，并拥有银行卡及三大运营商数据资源，可以与银行卡验证业务及运营商验证业务并行使用。总体验证成功率99.997%，系统响应速率平均450毫秒。

“你需要的是银行卡核验，就走的是银联的信息；如果需要身份证核验，走的就是公安部的。”上述银联业务负责人表示，相比NCIIC的5*8小时服务，银联提供的是7*24小时的服务，价格最低可以到每次查询两毛钱左右。

他透露，接入银联接口的主要是银行、证券、保险、政府机构以及一些大型互联网公司，也有一些很小的App可能会找银联的代理商。

谈及直联银联的优势，他表示“会比较便宜”，因为二级数据代理商“可能有一些溢价”。

但南都记者调查发现，事实并非如他所说。

上述银联业务负责人对南都记者说，银联“很少会去做直拓”，除非客户直接打电话过来询问，否则大部分情况下都是由银联的合作伙伴（二级数据代理商）去进行拓展。

国有数据资产增值运营服务商“数据宝”也曾在知乎上作答称，公安系统的官方渠

道“基本都不做直客”，而是经由授权服务商对外提供——数据宝就是其中之一。想要拿到官方授权，服务商必须要有信息保障的安全体系。

二级数据代理商没有一手数据，收到核验需求后，它们会将其提交给最上游的官方数据源，并将收到的比对结果返回给客
户。
由于公安系统、运营商和银联的合作门槛普遍较高，市场上最活跃的正是这些二级数据代理商。

数据科技服务商“聚合数据”扮演的就是上述银联业务负责人口中二级“数据代理商”的角色。

聚合数据客服告诉南都记者，身份核验的数据来源主要是公安部。“相当于咱们聚合数据是一个中转站，把诉求发到公安部，然后得出一个‘一致’或者‘不一致’的结果）”，他说，“我们相当于一个中间商赚点差价”。

聚合数据官网上显示，如果一次性购买的查询次数达到四万次，价格可以便宜到每次两毛钱。如果查询次数达到十万，该客服称还可以便宜到每次一毛钱。

值得注意的是，上述银联业务负责人所推测的“溢价”并未出现，甚至购买聚合数据的接口还会更便宜。

类似情况也出现在了一个下游数据接口服务商上。

这类数据接口服务商往往不具备直联一级渠道的资质，但长处在于能灵活调整解决方案，满足各行业终端用户五花八门的应用场景。于是，他们在二级数据代理商和终端用户之间充当起“N道贩子”，查询接口也因此被层层转接。

尽管“接口简介”中称实时联网NCIIC，但该数据接口服务商的销售人员透露，“我们是跟上游商业公司合作的，他们直联公安系统。”按照这个说法，数据的返回路径应该是：公安部-上游商业公司-数据接口服务商-用户。

依照常识来看，两级中转会大大降低系统响应速率，但他表示“一般（每次查询）100毫秒左右都可以完成的”，因为“我们服务器的优化这块做得比较好”。

除了响应速率更快，该数据接口服务商“身份证验证”业务的价格也比聚合数据更便宜。只要一次性购买的查询次数上万，就能享受每次低于两毛钱的价格；购买超过五万次，价格最低可以到每次一毛三。

南都记者注意到，根据数据宝的知乎回答，如果接口每次查询价格低于一毛钱，响应速率快至200毫秒以下，且对个人用户开放，极有可能是非法缓存或买卖其他机构缓存所得的数据。

业内通用

所谓“缓存”，是指查询接口提供商将获得的身份核验信息存储在本地。它就是为什么“理论上应该是越远离数据源的价格越高、系统响应速率越慢，但现实却恰恰相反”的关键所在。

按照法律要求，这些提供商不直接对接个人用户，无权存储公民个人信息。但是不少提供商都会悄悄缓存数据，然后提供相关数据服务。当累积的数量足够多，这笔生意可谓“一本万利”。

据了解，
很多数据接口服务商的缓存数据来源不仅来自于上游，也来自于下游：当下游提交需要核验的个人信息时，进行缓存；当上游返回的结果为“一致”，则相当于拥有了一条真实数据。

长此以往，大量真实的公民个人信息会形成一个缓存数据库。之后再收到核验需求时，数据接口服务商只需直接跟缓存数据库里的信息进行比对，如果有，直接返回结果即可；如果没有，再返回到上级数据源，进行付费比对。

多位业内人士告诉南都记者，缓存“是业内的一个通用做法”。还有业内人士估计，目前国内有8亿元的缓存量市场。

有了缓存数据库，数据接口服务商就可以省掉不少调用上游数据源的费用，从而削减成本，压低对外提供查询接口的价格。而大量的公民个人信息则未经本人允许，被非法存储在了官方授权渠道之外，个人信息泄露的源头也就从此开始。

去年，拉卡拉支付旗下的考拉征信就因违规出卖从上游公司获取的身份信息查询接口，非法缓存公民个人身份信息被查。下游公司从考拉征信购买查询接口后以此牟利，造成了公民身份信息包括身份证照片的大量泄露。

暗地操作

既然非法缓存已经是业内众所周知的“黑灰产”，为什么二级数据代理商依然愿意“冒险”将接口转卖给下游数据接口服务商？

就此，南都记者假称有身份信息核验的需求，且可能需要把查询接口共享给第三方的关联公司或合作伙伴，联系了数个二级数据代理商。

聚合数据客服称，与接入公司签订的合同肯定会明确查询接口不能转售，但是至于“对方私下有没有按照合同操作，就和聚合数据没有关系了……打个比方，你买了我的菜刀，然后去街上砍了人，肯定不能怪我卖菜刀的对吧？”

另一家数据代理商用友APILink给南都记者发来了合同。合同条款明确：“甲方为购买‘用友云’应用服务的唯一合法使用者，未经乙方（用友）书面同意不得将本合同项下服务授权第三方使用”。

但当南都记者询问是否可以与第三方共享数据时，洽谈业务的用友负责人称，虽然不鼓励这么做，但即使做了用友也监控不到。

不过，无论是二级数据代理商还是更下游的数据接口服务商都向南都记者表示，绝对不会缓存数据。

他们还透露，考拉征信出事之后，查询接口买卖也有所收紧——最明显的变化是多个查询接口提供商都提高了对接入公司资质的要求。

“我们这块业务只面向一些企业去开放。有一些灰色地带的企业，目前我们没办法进行合作，比如说P2P之类的。”用友负责人强调。聚合数据客服也提到，必须认定对方产品合规才允许接入。

前文提到的数据接口服务商则已经接到了上游数据接口服务商的通知，要求其2020年起“切断没有资质的接口”，即不能再把接口提供给第三方公司。“以后我们也只能自己用”，销售人员说。

由此看来，上游的数据代理商并非对接口转卖、非法缓存完全不知情，但他们选择了“睁一只眼闭一只眼”。

随着《中华人民共和国网络安全法》的出台，以及考拉征信等金融科技公司出事，他们或许才开始正视公民个人信息可能因此泄露一事。

上述曾在运营商工作的专家对此感触颇深。“在（考拉征信）出事之前，2018年很多（公司）都明目张胆地出售身份信息查询接口……2019年少了很多，以后还会少很多。”

如何规范？

尽管引起行业震荡的考拉征信被查一案尚未公布调查结果，但在已经审结的案件中，利用查询接口获取公民个人信息牟利的行为已有先例。

2017年，被告方某、徐某用成立车盾科技成都有限公司（下称“车盾公司”）后，向山西晟盾信息科技有限公司（下称“晟盾公司”）等购买公民个人信息查询接口，共查询公民个人信息7万余条，并由此获利17万余元 。

法院判定，车盾公司获取公民个人信息时，没有法律依据或正当理由，既未得到公安机关或任何部门的许可，也未经过当事人授权。因此分别判处两名被告有期徒刑三年和有期徒刑一年。

在类似案件中，法院作出判定的理由是“非法获取公民个人信息，并向他人出售”。实际上，目前不少相关法律法规对此都有规定。

> 网络安全法第四十二规定，未经被收集者同意，不得向他人提供个人信息；第四十四条规定，任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。
>
> 根据《最高人民法院、最高人民检察院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》，违反国家有关规定，通过购买、收受、交换等方式获取公民个人信息，或者在履行职责、提供服务过程中收集公民个人信息的，都属于“非法获取公民个人信息”。

多名专家对南都记者表示，目前法律上对谁有资格提供身份信息核验服务的规定并不明确，但如果各级数据服务商都能做到合规，并不必然导致个人信息泄露。

问题出在“非法缓存”公民个人信息并以此牟利的行为上。

“这个接口本身实际上只是提供查询服务的一种方式，法律上没有禁止”，对外经济贸易大学数字经济与法律创新研究中心执行主任许可指出，“而且这些数据本身是用户提供的，公安部只是做了一个是或否的回复，不存在数据传输。”

他表示，
数据服务商与终端用户之间没有直接关系，应该在按照委托人指定的目的做完身份核验之后就删除数据，无权长期存储这些数据或用于其他用途。如果导致个人信息泄露，应该由当事企业承担责任。

谈及数据接口服务商对于接入企业的监管责任，上海金融与法律研究院院长傅蔚冈

认为，双方应该遵循网络安全法签订严格的协议，确保数据不会大面积泄露；数据接口服务商还应该具备一定的安全技术，保证接口不被盗用。

查询接口层层转接，数据接口服务商资质参差不齐、非法缓存无人监管，都为公民个人信息泄露埋下了极大的隐患。如此混乱的身份信息核验市场该如何规范？

许可认为，身份信息属于公共数据，身份信息核验是国家提供的基础服务，不应交给第三方来运营，也不应该收费。在目前已经免费的基础上，公安部等一级渠道可以建立准入标准，允许有资质的企业接入，不再下设代理商。

接入企业的数量放开之后，考虑到可能需要针对不同应用场景产生开发成本，或者造成数据源端口的流量拥堵，也可以适当收费。这时多个企业或机构会相互竞争，不至于形成垄断，价格也会更加合理。

傅蔚冈也建议，可以从数据源头上开放多个渠道，把纵向的身份信息核验链条变为横向，让其他有资质、有能力的机构和企业把手上的资源利用起来，这样价格就会降下来，而不是层层加码、衍生出“旁门左道”。

从数据安全监管的角度，中国信息安全研究院副院长左晓栋提出，目前的监管还停留在表面上，技术分析能力不足，还不能有效地发现非法缓存等违规行为，但并不意味着将来也做不到。他建议，监管的下一步应该深入到企业具体内部行为、后台行为上去。

采写：南都记者蒋琳