个人信息贩卖已形成一条完整的产业链，且已由国内转向国外的网络空间。在这个空间里，一个人重要的隐私信息几乎暴露无遗，身份证号、家庭住址、车牌号、手机号、住宿记录，全部“上架”待售

Telegram平台上出售个人信息的群组截图

那么，这些只要付费就可以随意查询的个人信息都是从哪里来的呢？

《财经》记者询问一些卖家，对方称，
信息是从互联网各处“收集”而来。前述知情人士则认为，这些信息有不少是从历次泄露事件中整合而来，也有黑客会继续窃取，使得数据库的规模不断扩大。

《财经》记者经过亲身体验发现，具体交易流程并不复杂，找到机器人，买家充值获得积分后，可以直接用积分进行自动查询。

《财经》记者购买一些比特币，向机器人支付获取了积分。为了测试信息的准确性，《财经》记者向机器人发送了10个近亲属及朋友的手机号码，并支付10个或20个积分进行“绑定查询”，
仅3秒左右时间，机器人提供出查询结果。在这10个号码中，有9个手机机主的名字准确无误。
其中还有一个号码查询到准确的微信账号名和微博账号名，另有一个号码则准确查询到一位朋友使用过的邮箱密码和家庭住址。

在Telegram的此类群组中，手机机主信息只是一个入门级别的查询。《财经》记者使用机器人提供的“猎魔查询”（模糊搜索）功能，向其发送一个亲友的名字，随即机器人提示选择男女和省份。在支付100积分后，得到近30条与这名亲友同名的身份证号码信息，记者的亲友也位列其中，且身份证号码准确。

前述知情人士称，“猎魔查询”可以被用于“人肉搜索”，只需要提供被“人肉”的人的名字，就可以通过不同的信息，一步步精准锁定搜索对象。

除了查询和出售业务，《财经》记者还联络了群组中一些出售信息的卖家。记者向一名卖家提供身份证号，表示想查询这个身份证号的住宿信息。卖家表示，此类信息是以一个数据包的形式出售，数据包中包括少则数万条，多则几百万条信息，价格也从几百到几千元不等。

这位卖家称，数据包越大，就能查到越多的准确信息。在买到的一个数据包中，《财经》记者通过身份证号码查询，果真得到几条准确的住宿信息。但住宿时间并不是最新的，基本为2018年以前的信息。

因为机器人充当了第三方的角色，透过机器人查询购买，得到信息的准确性强、可靠性高，不存在传统平台上付款后被卖家拉黑的情况。这对于诸多买家来说，无疑是一种“高品质”而又可靠的服务。

前述知情人士对《财经》记者表示，新的销售方式方便了黑灰产的从业者“开展业务”，这些信息贩子
隐匿于平台背后，追踪溯源的难度增大。
同时，个人信息贩子预先购置了大量黑灰产“四件套”——身份证、银行卡、手机号、U盾，用以提现。

为了保证安全，
“四件套”均非使用者本人信息，而是从另一批专业黑灰产人士那里购得。由此可见，个人信息贩子已非单链条发展，已经发展成为产业网络。

同时，信息贩子利用数字货币交易的特性，可以为每个卖家单独生成地址，以便于交易“安全”和隐匿交易痕迹。

经过多日调查，以及一些知情人士提供的信息，《财经》记者初步掌握这一黑灰产业链条，上游为一些黑客为代表的技术人员，他们通过各类手段获取海量数据。中游即为各类信息贩子，他们从上游购买获取数据，在群组内出售。

购买者根据自身需求购买数据和信息。据知情人士透露，这些购买者主要为三类群体：
网贷从业者，购买个人信息用于向借款者追讨借款；私家侦探，购买查询信息用于调查业务；还有一部分散户并无具体目的，把购买、查询自己想要的某个个人的信息当作一种心理需求。

Telegram为何成黑灰产“温床”？

令人觉得讽刺的是，有众多个人隐私信息被交易的网络平台——Telegram，其实是一款对待用户隐私和信息安全高于一切的产品。

2006年，帕维尔·杜罗夫和他哥哥一同创建了俄罗斯版的Facebook——VKontakte。2008年,VK用户超过1000万，成为俄罗斯最大的社交网站，估值达到3亿美元。

2014年，帕维尔因拒绝向俄罗斯政府提交乌克兰反对派数据、关闭俄罗斯反对党领袖页面的要求，被迫离开VKontakte。之后，他和哥哥前往美国纽约州，在那里与团队一起开发了即时加密通讯软件 Telegram。

简单来说，Telegram有一个绝对安全的加密信息传输网络，支持端对端加密。此外，Telegram 提供阅后即焚、私密聊天等功能，可以满足用户保护隐私的需要。

起初，Telegram曾提供了一项功能，即允许用户通过上传电话号码来搜索其他用户，以便让新用户快速了解手机通讯录中的人是否已经在使用这款软件。这项功能会自动将电话号码与群组中的用户名匹配起来，若执法部门向当地电信服务部门询问电话号码的持有者，就可以知道用户的真实身份。

后来，Telegram发布更新，允许用户禁用电话号码匹配。这样就增大了锁定使用者身份的难度，以此增强了私密性。在这样的平台规则下，Telegram的群组可自由进入，但用户信息全部很好地得到隐藏。

符合用户期待的隐私理念，安全快速的产品体验，让Telegram迅速得到发展。2018年3月，Telegram宣布其全球用户已超过2亿，每天发送120亿条消息。一年后，

其用户数量超过3亿。

然而，也正是基于这样的私密特性，以及可提供虚拟货币交易的功能，致使大量非法交易纷纷在Telegram里出现，包括一些军火交易、色情交易，甚至被恐怖主义组织利用。也就能够理解，Telegram为什么会成为个人信息贩子们的乐土。

在近期轰动韩国的“N号房”事件中，同样涉及Telegram。“N号房”运营者在Telegram上建立按等级付费的私密聊天室，供会员分享女性甚至未成年女被性剥削的照片和视频。

出于绝对保护用户隐私的理念，Telegram拒绝向俄罗斯联邦安全局提供用户加密信息，2018年4月，俄罗斯联邦电信、信息技术和大众传媒监管局宣布全国封锁Telegram。此后，Telegram又在俄罗斯以外的多个国家被禁用。

被“人肉”的调查者

今年29岁的佟林，长期从事数字货币、网络安全等业务，对这些领域的情况轻车熟路。

3月20日左右，微博用户个人信息泄露的消息发出后不久，出于公益目的，佟林立刻潜入前述Telegram群组，观察群组内的活动动态。

佟林接受《财经》记者采访时表示，他其实早已听说，网络黑灰产人士从国内网络平台转往国外平台，这在圈子里并不是秘密，只是普通公众一直尚不知情。

在“潜伏”多日，并尝试着与卖家交易后，佟林将这一类系列情况发布在自己的自媒体平台上，很短时间就获得将近10万的阅读量。

就在佟林继续“潜伏”时，他发现了一个叫“佟林粉丝”的群组，他进群后发现，自己已经被里面的诸多卖家“人肉”了。
他的名字、电话、家庭住址、工作机构等个人信息被准确无误地公布出来。连他的身份证原件图片也被晒了出来。
有人还威胁要使用电话、短信骚扰软件对他进行“狂轰滥炸”，彻底“废”了他。

面对这样的报复，佟林没有选择沉默，将自己被“人肉”的情况继续发布在自媒体中，并根据自己的互联网安全经验，提示普通公众在使用互联网时，可以采取一些办法保护自己的个人信息。例如，尽量少使用同一个密码或密码关键词；使用强密码管理工具，为账号开启二次验证；注册使用多个邮箱，有时也可以使用一次性邮箱等等。

佟林告诉《财经》记者，
前述Telegram群组中的卖家所提供的个人信息中，很多都是被用于“人肉搜索”。而在这些群组中，真实
个人信息公开被称为“出道”。
在佟林看来，自己个人信息的完全泄露，已经意味着任何一个个人都可能已经失去了应有的隐私空间。

佟林对《财经》记者表示，自己既然已经“出道”，就愿意用自己的经历将这些侵犯个人信息的情况更大范围地让公众知晓。但有一点最让他始终难以理解，那就是自己的身份证原件照片也被泄露出来了，“这种应该是管理最为严格的信息，怎么也就这么泄露出来？”

《财经》记者在上述群组中注意到，
群内成员对于各类揭露类似个人信息贩卖的报道反应速度极快，报道刊发后不久就会被转到群内，群内成员对这些报道不以为然，发表各类嘲讽，甚至声称会去“人肉”记者。

信息泄露的源头能堵住吗？

个人信息泄露事件近年来屡有发生，已对普通公众产生滋扰，最常见的是很多人经常会接到各类精准营销。而一些由于电信诈骗案件引发的恶性事件更是让公众感到不安。

很多人都存在疑问：个人信息究竟是如何泄露的？究竟有没有办法防止泄露？

中国电子技术标准化研究院信安中心审查部总监何延哲告诉《财经》记者，近几年的个人信息泄露，一般有三个来源。一是“黑客”等外部力量攻击数据库，用技术手段把内部信息盗走；二是存储有海量数据的机构，有内部人员利用系统管理权限将数据获取后流出；三是在使用第三方网络平台时，用户将个人信息提交给平台，但这些平台的防护措施不到位或没有按照约定存储使用数据，导致泄露。

针对这三种情况，想防止数据泄露，掌握海量数据的机构应该加强技术防护，制定严格管理制度，同时严防“内鬼”。
出于对数据安全的考虑，各机构也都在加强防护措施，但在现实中并不可能做到完全没有漏洞。

何延哲向《财经》记者举例，从2019年开始，中央网信办、工信部、公安部、市场监管总局四部门联合展开App个人信息保护治理，对不断提升App个人信息保护水平起到了积极推动作用。但是只要出现一个“内鬼”，大规模泄露立刻出现，防不

胜防。

以酒店住宿信息为例，近两年已有多起大规模泄露事件。

2018年8月，华住酒店集团发生泄露事件，涉及的个人信息数量超过5亿条。华住旗下的酒店品牌包括汉庭、美爵、桔子、全季、宜必思等，门店数量数千家。

2018年12月，国际酒店巨头万豪对外披露，其旗下品牌酒店的客人入住信息系统遭黑客入侵，数亿条个人入住信息和身份信息被泄露。

就在2020年3月末，万豪再次公告称，约520万名客户的资料可能被泄露。这次泄露的原因则为可能有人使用集团旗下一家特许经营酒店的两个员工的登录凭据，访问了数量众多的客户信息。万豪方面发现后，已禁用相关登录凭据，并通知有关部门展开调查。

检索中国裁判文书网可知，顺丰速运曾发生的一起内部员工泄露个人信息的案件。这是近年来快递行业涉及泄露个人信息的一起重大案件。

湖北省荆州中级法院2018年5月的一份判决书显示，顺丰速运员工杜立明、冯丹等11人分别就职于河北顺丰速运有限公司和荆州顺丰速运有限公司，职位涵盖安保部主管、市场部专员、仓管、快递员等。

2015年以来，杜、冯等人为谋取非法利益，利用微信、QQ等软件平台，出售、提供、非法获取包含顺丰快递单号、面单（即包含顺丰快递单号、地址、电话号码的图片）中公民的个人信息。案件涉及被泄露的公民个人信息超过千万条，涉案金额200余万元。如果折合成单条信息，每条价格仅有约0.2元。

除了酒店业、快递业，同样掌握有海量数据的一些行政机关工作人员也成为个人信息泄露的“内鬼”。

2020年4月初，湖南省衡阳市公安局刑侦支队五大队原民警肖某二审获刑四年半。衡阳中院判决认定，2017年3月，肖某发现出售公民个人信息可以赚钱，便开始利用职务便利，出售个人信息牟利。

由于肖某自己的数字证书无高级查询权限，他盗用同事的数字证书，通过登录公安机关相关信息平台，将查询到的公民户籍信息或行踪轨迹信息出售。肖某先后出售过的个人信息包括公民户籍信息、公民个人行踪轨迹信息、车辆轨迹信息、住宿信息。他设定的价格为公民个人行踪轨迹信息每条300元，车辆轨迹信息每条100元，住宿信息每条100元。

在交易过程中，肖某曾使用国内软件进行交易。出于安全考虑，他也改用一些国外软件进行联络和交易。法院审理认定，自2017年3月至2018年12月，肖某盗取公民个人信息出售给他人，违法所得总计180余万元。

正是由于国内对于信息泄露和贩卖等非法行为的治理，这些黑灰产从业者转移到Telegram这样的国外平台，以逃避打击。

截至发稿时，前述Telegram群组的参与人数仍处于不断增长中，而各种个人信息交易依然活跃。