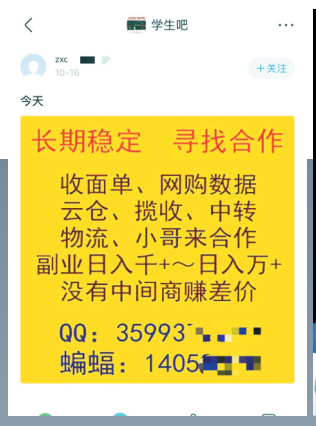

一名收“快递面单”的用户发帖寻觅卖家。网页截图

“卧底”快递公司的嫌犯用手机拍摄面单上的个人信息。　视频截图

我国首部《个人信息保护法》施行 买卖个人信息最高判刑7年

嫌犯“卧底”快递公司偷拍倒卖个人信息

《个人信息保护法》11月1日起正式施行，这是我国首部专门针对个人信息保护的系统性、综合性法律，其中明确：不得过度收集个人信息、滥用人脸识别技术、大数据杀熟等。随着法律法规的日益健全，公安机关也不断加大对侵犯个人信息犯罪的打击力度。但是，依然有不法分子铤而走险窃取公民个人信息。事实上，在这部专门性法律出台前，已有不少个人信息保护条款散见于诸多法律之中，多地法院也已有过大量司法实践。

值此重大节点，记者以“侵犯公民个人信息”、“买卖公民个人信息”等关键词，在裁判文书网上获取了8602份判决书，以此观察2016年至今相关案件的数量分布、涉案信息量、涉案金额和量刑趋势等。分析结果显示，相关文书数量在2019年达到顶峰，其中超半数个人信息从行业内部工作人员处泄露。在这些“内鬼”中，有近四分之一出自公安系统。此外，泄露的个人信息类型极广，从新生儿信息、股民信息到开房记录，无所不包。

姓名和电话最常泄露 主要被用于贩卖牟利

《个人信息保护法》规定，个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，而此前的《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》（下称《两高司法解释》）则对公民个人信息做出了更详细的定义，其中包括姓名、身份证件号码、通信联系方式、住址、账号密码、财产状况、行踪轨迹等。

8000多份文书中，最常见的涉案个人信息是姓名和联系电话——它们出现在了半数的案件中。紧随其后的是身份证信息、居住地址和车辆信息。值得注意的是，在泄露的车辆信息中有31.08%来自公安系统，而20.79%的居住地址从房地产公司和快递公司泄露。

此外，部分涉案数据针对特殊群体，如新生儿和股民。此类数据往往直接从相关从业者手中流出，买家购买数据的主要诉求通常是有针对性地推销或诈骗。

以文书（2017）沪01刑终525号为例，2014至2016年，就职于上海疾控中心的韩某利用其工作便利，进入他人账户窃取全市新生婴儿信息，每半个月向其下家张某发送约5000条信息。张某获取信息后，又转卖给专做婴幼儿保健品生意的范某。直至案发，韩某、张某、范某累计非法获取新生婴儿信息共计20余万条。

在上述案件中，信息的泄露、买卖属于产业链的上游。事实上，随之而来的推销、诈骗等对普通人的影响更大。

在记者分析的8602份文书中，有6949份提到了被告人在获得数据后的用途。而在一份文书中，可能出现多个被告人，因此数据可能会有多种用途。其中，大部分被告人选择直接贩卖数据牟利，占79.77%。此外，34.36%被用于推广，10.48%则和诈骗相关。

除了对人们生活和财产的侵犯外，个人信息的泄露甚至会对人身安全造成威胁。

报复类案件在所有文书中只出现了8次，占比仅为0.1%，但对每一个受害者来说，却可能是一生挥之不去的阴影。

网上售卖“料”“菜” 实时面单抢手

快递面单，是快递公司在送货时用来记录发件人、收件人、货物种类、价格等相关信息的单据，需要贴在快递包裹上。一张快递面单，包含了收件人的姓名、电话、家庭住址等隐私信息。记者调查发现，目前这些快递面单在网上被明码标价批量售卖。

记者试着在百度贴吧输入“快递”“面单”等关键词，出现很多相关分类群组。而为了逃避打击，不法分子会使用一些暗语来代替，快递信息通常被称为“料”“菜”等。

在“快递吧”，一个网名os开头的人打出“收菜，来中介对接”的广告，并留下一个联系方式；另外还有人打出“工作室对接，出历史，可测试”的广告。据记者了解，快递面单被收购者分为“实时”和“历史”两种，而实时面单是最抢手的“货源”。

记者通过一款即时通信软件联系了多名买家，其中一个叫“橘子”的人报价：实时面单超过1000张的话每张价格3.5元，精品面单每张4元；而历史面单只收车载、童装童鞋、化妆品类的，每张1.5元。

记者又联系了一名卖家，这个叫“悟空”的人声称，自己手里有几十万张历史快递面单，货源是一家物流“云仓”。当记者表示要验货时，对方发来多张面单图片，上面有消费者详细的个人信息。为了证明自己的实力，他还给记者发了一份文档，里面按照化妆品、母婴、服装等分门别类，其中包括上百位消费者的姓名、所购商品、家庭住址和电话号码等隐私信息，甚至还有商品的价格。据网络安全专家万仁国介绍，消费者下单购买商品的当天，快递信息可能就已经被卖掉了。

临时应聘入职 获取信息牟利

那么，都是谁在贩卖公民个人信息呢？数据显示，行业内部人员——也就是俗称的“内鬼”占了大多数。

2017年，公安部网络技术研发中心主任许剑卓曾表示，行业内部人员已经成为侵犯公民个人信息犯罪的主体。他指出，从治理犯罪来说，打击源头是最重要的工作。而在2018至2020年的“净网行动”中，公安机关抓获侵犯公民信息的行业“内鬼”3000余名，在“净网2021”专项行动中抓获行业“内鬼”500余名。

值得注意的是，在记者获取的8000余份文书中，近四分之一的“内鬼”来自公安机关内部。一般而言，公安内部人员能接触到的敏感个人信息更多，诸如家庭住址、车辆、行踪轨迹、开房记录、犯罪记录等。数据显示，大部分“内鬼”从属于基层派出所和交警大队，这其中又以辅警和协警居多——虽然这些“编外人员”权限较低，但他们可以通过盗用正式干警的数字证书，或通过用他们的账号密码登录公安内网等方式获取数据。此外，也有文书表明，有些干警是自己把数字证书权限交予“内鬼”的。

涉及“内鬼”的信息往往和其对应的“专业领域”有着强关联。房地产工作人员主要贩卖的是业主、小区信息，银行从业人员则“主营”股民、贷款和账户信息。而不同专业领域又导向了不同的犯罪类型——从电信公司工作人员手中流出去的数据常被用于电信诈骗和推广，从各个渠道中流出的贷款相关数据则和网络放贷业务有关联。

今年9月初，浙江省宁波市北仑区一家进口外贸公司报警称，公司陆续收到消费者的投诉电话，称大量个人信息泄露，已经有客户被诈骗。

据警方了解，这个犯罪团伙为了获取快递包含的个人信息非法牟利，竟然通过临时应聘的方式进入快递公司。他们利用整理快递包裹之机，偷拍快递面单照片，汇总整理后在网上倒卖。

在掌握大量线索后，宁波警方开展了抓捕行动，先后抓获犯罪嫌疑人9名，查获快递面单照片2万余张。

除“内鬼”外，通过购买、交换等方式获取公民个人信息的案件也不在少数，这说明公民个人信息的买卖市场仍然不容小觑，一条数据可能经手多人，被“多次利用”。其中，不少案例中的被告人假借“信息咨询公司”之名从事个人信息买卖犯罪。跟踪、偷拍的数据虽相对较少，但多为针对特定个人、达成特定目的实施的犯罪，实际威胁性非常大。

隐私面单早有 为何没有普及

快递行业早在2017年就推出隐私面单服务，与常规面单相比，隐私面单能把用户的关键个人信息用二维码或星号隐藏起来，基本可以保证个人信息不被泄露。但是，目前隐私面单却一直没有大范围使用，这是为什么呢？

对此，专家介绍，一方面是由于部分用户在寄送快递时没有意识勾选或使用不便；另一方面，使用隐私面单也会给快递员增加额外工作量。

中国政法大学传播法研究中心副主任朱巍认为，最主要的还是考虑成本问题。因为现在快递业发展比较快，如果用隐私面单的话，需要专门的终端识别设备。另外，隐私面单需要扫码才能完全显示，快递效率可能较低。《个人信息保护法》在个人信息处理者义务里面特别提到，处理个人信息时，应当对个人信息进行相关操作，像加密、去标识化，这是基本的安全技术保障措施。以前隐私面单可能是平台提供发服务，现在就变成了一种法定的义务。

筑牢信息屏障 提供全面保护

据中国互联网络信息中心数据统计，截至今年6月份，我国网民总体规模超过10亿，网站数量和App数量分别超过422万个和302万款。在信息化时代，信息保护成为大家最关心、最直接和最现实的问题。11月1日，我国首部《个人信息保护法》正式实施，记者就一些问题采访了法律专家岳屾山。

有法无法，区别在哪？岳屾山认为，《个人信息保护法》筑牢了信息保护屏障，也提供了细致全面的保护。首先，《个人信息保护法》是一部专门的个人信息保护立法；其次，《个人信息保护法》明确了相关主体的权利和义务；再次，《个人信息保护法》为相关部门处罚侵犯公民个人信息违法行为提供了明确的法律依据和标准；另外，《个人信息保护法》大幅度提高了侵犯公民个人信息违法成本等。

侵犯个人信息，后果如何？岳屾山表示，买卖个人信息，最高可处7年有期徒刑。公民的个人信息受法律保护，包括但不限于公民的姓名、身份证号、电话、住址、生物识别信息以及行踪轨迹等。我国刑法规定，不管出售、购买还是窃取个人信息，达到一定标准都会构成侵犯公民个人信息罪。

据央视、《南方都市报》