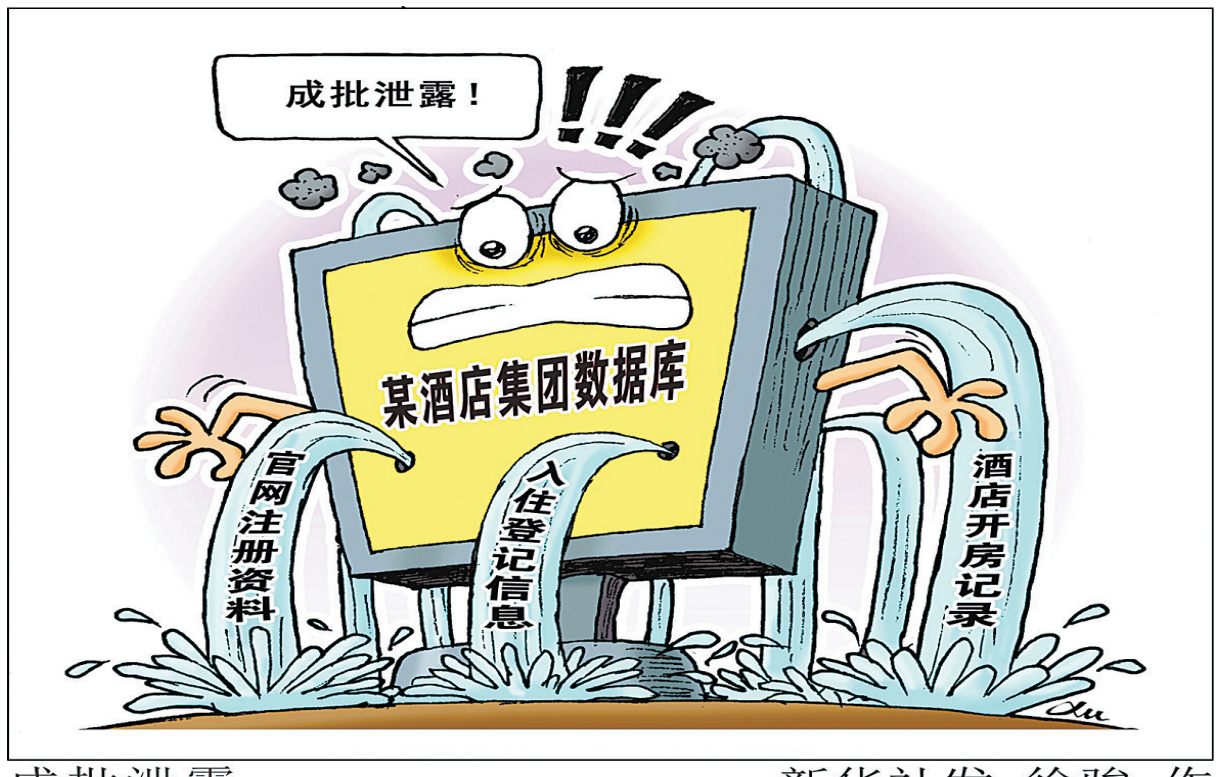
5亿条个人信息在网上出售

四问“华住”开房记录成批泄露事件

“每10个国人，就有一个‘住’客。”在华住酒店集团官网上，这样的广告宣传语在首页滚动播放，这与网帖中所“挂售”的1.3亿人身份证信息“不谋而合”。

8月28日，网络流传一张黑客出售华住酒店集团客户数据的截图，其中涉及姓名、身份证号、家庭住址、开房记录等众多敏感信息，大约5亿条，全部信息打包价为8比特币——约38万元人民币，并给出了测试数据。针对公众关注的几个焦点问题，记者采访了业内人士与专家。



成批泄露　　新华社发　徐骏　作

“华住”开房记录成批泄露

作为世界排名第九的酒店集团，从快捷酒店起家的华住集团，现在已在370个城市拥有3700多家酒店，旗下酒店包括美爵、禧玥、漫心、诺富特、美居、CitiGo、桔子、全季、星程、宜必思、怡莱、海友酒店等。据网络消息，泄露的个人信息截止到今年8月中旬。

8月28日凌晨6时，某中文论坛中突然出现一条题为《华住旗下酒店开房数据（汉庭、桔子、全季等）》的数据出售帖。在该帖的出售数据中，包含姓名、手机号、邮箱、身份证号等网站登录信息约1.23亿条；包含姓名、身份证号、家庭住址等约1.3亿人身份证信息；包含姓名、入住时间、离开时间、房间号、消费金额等开房记录约2.4亿条。上述信息的打包售价为8比特币或520门罗币（约合人民币38万元）。

为了取信买家，发帖人还“附送”了约3万条的样本数据，供买家核实。有媒体对样本数据进行抽样比对后发现，该数据与真实信息吻合度较高。

网络安全专家高天分析认为，华住集团的开发人员将敏感信息数据库上传到了GitHub（该网站为公开代码托管库，通常程序员将未完成的代码上传至该网站，以便日后继续编辑），是导致此次信息泄露的主要原因。记者了解到，发帖人还声称，“如果权限不丢失，后续数据还可以免费发给已购买者。”截至记者29日15时发稿时，该帖的样本数据显示已有4572次直接下载量，但尚未有人完成交易。

今年以来，国内多家机构疑似发生数据库泄露事件。6月13日，知名视频播放网站A站（AcFun）遭遇黑客攻击，数据库近千万条用户数据发生泄露；6月14日，前程无忧数据库195万余条用户数据疑似泄露，但遭该公司声明否认；8月1日，浙江省1000万条学籍数据疑似泄露，样本数据经核实与真实信息基本一致……

网络安全专家表示，当前隐私信息泄露呈高发态势，这些个人信息可被不法分子用以实施精准诈骗，而诸如开房记录等敏感信息外泄，则有可能诱发针对个人的敲诈勒索等犯罪行为。

一问　天量信息泄漏可能产生哪些危害？

“华住5亿条个人信息疑似泄露”事件引发广泛关注，目前警方已经介入调查。针对公众关注的几个焦点问题，记者采访了业内人士与专家。

华住酒店集团公关负责人魏佳29日对记者表示，公司正在积极配合警方调查。如有最新进展将及时披露。华住酒店集团已在企业内部迅速开展核查，并第一时间报警；公司也聘请了专业技术公司对网上兜售的“相关个人信息”是否来源于华住集团进行核实。目前，上海长宁警方也已介入调查。

我国网络安全法对发生或者可能发生个人信息泄露、毁损、丢失的情况规定了法律义务。网络经营者应当立即采取补救措施，按照规定及时告知用户，向有关主管部门报告。

记者随机测试了7个测试数据中的电话号码，除了一个没有打通之外，其他号码与姓名都是相符的。有些测试对象表示近期确实入住过华住相关的酒店，还不知道个人信息已经泄露。这些个人信息被泄露可能产生什么风险？专家表示，可能会被用于多种场景，获取非法利益。

较早公布这一泄露消息的国内民间互联网组织“网络尖刀”团队创始人之一曲子龙分析，用户隐私数据泄露是一个特别多元的利益链，数据“黑市”由多种身份参与者组成：其中，订单信息泄露可能被不法分子用于“电信诈骗”；身份信息可能被不法分子冒用到一些审核不严谨的P2P或其他金融平台借贷；行为数据可能被一些违规营销公司做所谓的“大数据营销”；用户账户密码可能被不法分子用于在互联网上撞库攻击盗取新的数据信息。

二问　信息是从何种渠道泄露的？

目前，关于信息的泄露渠道尚在核查中。曲子龙29日向记者表示，数据是否泄露、如果泄露具体因何引起，目前都是通过手中有限的内容推断的，具体情况还要等警方调查、华住集团核查的结果出来后才能得知。

据介绍，信息泄露的主要渠道有三种：企业或外包公司安全意识不足，导致系统安全体系不完善；内部员工或离职员工主动泄漏；黑客恶意攻击。

研究机构发布的《2018网络黑灰产治理研究报告》指出，“网络黑灰产”每天都会发起17亿次的恶意访问试图窃取数据。

根据360补天漏洞相应平台的数据，仅2017年1月至10月，共收录可导致信息泄露的网站漏洞251个，涉及网站150个，共可能泄露信息51.2亿条。

不少专家认为，目前，一些互联网企业和正处于信息化转型的传统公司，用户信息高度聚集，但安全意识没能同步升级。“我们遇到的绝大多数个人信息泄露，都是管理过失和主观错误。很多传统机构缺乏足够的网络安全技术能力，建设过程中甚至想不到这个问题，网络安全没有做到同步规划、同步建设、同步运营。”360首席反诈骗专家裴智勇说，“‘门’锁得紧紧的都很可能被黑客攻进来，更何况把‘门’打开”。

三问　信息一旦泄露如何尽量减少损失？

个人信息被泄露了损失能够挽回吗？专家介绍，与其他物品被盗相比，个人信息一旦泄露，理论上可以进行无限复制，只要有任意一个拥有者继续传播，就无法彻底追回。

专家说，通过修改密码，可以减少更多信息被泄露的可能性。有华住账号的用户，可以立即修改账号密码；如果多个网站都使用同一个密码，和华住一样密码的网站密码也应同步修改。

对于公司来说，必须切实加强网络信息安全建设投入，加大对数据的加密行为、设置更为清晰的隐私策略和权限，重要数据库只允许内网访问。

“打比方，大家都装起了护栏你却没有，那你就成为黑客攻击目标。大家都没有护栏而你有，黑客就会转移目标。”裴智勇说。

四问　如何避免类似情况再次发生？

涉及信息泄露的企业该负哪些法律责任？裴智勇说，如果网站此前接收到漏洞报告却没有及时主动处理，属于重大过失的，需要承担较大的法律责任；如果这个攻击技术是从未出现过的、业界任何人都防不住的，则法律责任相对较轻，“但后面这种情况很少见”。

多位专家表示，保护个人信息安全，不仅是企业的社会责任，更是法律义务。我国网络安全法规定，网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、损毁、丢失。专家认为，应加强对企业的监督和约束，倒逼其有效承担信息安全保护责任。

专家还认为，从源头收集端，加强防控和信息收集的规范是非常必要的。华东政法大学数据法律研究中心主任高富平表示，企业经营者收集、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。

《2018网络黑灰产治理研究报告》指出，由于犯罪技术更加平民化，黑灰产技术犯罪的成本正逐步降低。因此必须加大治理力度，坚决打击黑灰产。

专家提醒消费者一方面应利用法律手段保护自己，另一方面提高个人信息保护意识，慎重注册APP和扫二维码，提高密码设置难度，不同平台使用不同密码，并设置“字母＋数字＋符号”的加强密码，注意不定期修改密码。（新华社上海8月30日电）