个人信息安全保障能力建设研究

倪惠康[1],何　菲[2]

(1.上海市信息安全测评认证中心,上海 200011; 2.华东理工大学信息办,上海 200237)

摘　要:在互联网、大数据时代背景下,迅速发展的大数据信息系统对个人信息保护的要求不断提高,安全事件频发,从法律法规层面将个人信息保护提升到一个前所未有的高度。从个人信息泄露造成影响的现状出发,深入分析了个人信息的泄露源、泄露风险、泄露原因、泄露方式和泄露渠道。最后在各个方向上提出了对个人信息保护的解决措施,以纵深防护的思想让恶意人员无法获取个人信息、无法使用个人信息和无法逃脱法律惩戒。为加强信息系统个人信息保护能力提供参考。

关键词:数据安全;个人信息保护;信息泄露;电信诈骗

中图分类号:TP393　　**文献标识码**:A　　DOI:10.19358/j.issn.2096-5133.2020.02.004

引用格式:倪惠康,何菲.个人信息安全保障能力建设研究[J].信息技术与网络安全,2020,39(2):19-22,33.

Research on the guarantee ability of personal information security

Ni Huikang[1], He Fei[2]

(1. Shanghai Information Security Testing Evaluation and Certification Center, Shanghai 200011, China;
2. East China University of Science and Technology, Informatization Office, Shanghai 200237, China)

Abstract: In the age of Internet and big data, with the rapid development of big data information system, the high requirements for personal information protection are raising accordingly. From the perspective of existing laws and regulations as well as frequent happened security incidents, personal information protection has been promoted to an unprecedented height. In this paper, we deeply analyze the personal information leakage sources, risks, causes and ways. The related solutions are presented to protect personal information from all aspects, which can effectively prevent criminals from capturing and taking advantages of personal information. This research can take as a reference for further research of how to strengthen personal information protection ability in information system.

Key words: data security; personal information protection; information leakage; telecom fraud

0　引言

当今,互联网的大规模应用使得数据信息开始充斥于个人生活中,开启了整个社会的信息化数字化转型。互联网原本具有极强的匿名性,但当大数据时代来临,经年累月沉淀在互联网中的无数的个人信息性也变得不堪一击。个体被细化成为一个个数据包的集合体,被各种数据不停画像,最终将成为大数据时代的"透明人"。

个人信息保护问题在大数据时代里备受关注。在法律层面,2017 年 6 月《中华人民共和国网络安全法》正式实施[1],对个人信息保护问题给予极大关切;2018 年 9 月,《十三届全国人大常委会立法规划》已将个人信息保护法列入议事日程,相关立法呼之欲出;2019 年 6 月,国家互联网信息办发布《数据安全管理办法(征求意见稿)》[2],对"利用网络开展数据收集、存储、传输、处理、使用等活动"提出要求。在市场监督层面,2019 年 1 月中央网信办、工信部、公安部、市场监管总局等部门联合发布《关于开展 APP 违法违规收集使用个人信息专项治理的公告》[3],针对各类应用程序中存在强制授权、过度索权、超范围收集个人信息,违法违规使用个人信息等突出问题,展开全国范围的专项治理。

1　个人信息泄露造成广泛影响

个人信息泄露后造成的影响比较复杂,在各方面影响都呈耦合状,主要影响目前可以归纳为五类,后期随着智能化技术的发展,利用个人信息产生的影响将越来越大。一是商业环境下的广告精准投放。定向广告是互联网企业借助用户行为数

据分析目标用户的偏好或需求，进而针对不同类型的用户投放不同的广告。中国互联网协会发布的《2016 中国网民权益保护调查报告》表示，84% 的网民曾经遭受过因个人信息泄露带来的不良影响，比如广告推销等。二是电信精准诈骗。个人信息的泄露让犯罪份子实施精准诈骗有机可乘，根据中国银联公布相关数据显示，超过 90% 的电信诈骗是由于个人信息泄露引致的。三是互联网环境人肉搜索。人肉搜索一直是法律的灰色地带，其途径主要依靠个人信息泄露，对社会和个人造成一定的影响。四是账号密码泄露造成经济损失。2018 年底发布的《网络空间安全蓝皮书：中国网络空间安全发展报告（2018）》显示，从 2017 年下半年到 2018 年上半年，网民因个人信息泄露等造成的经济损失高达上千亿元。五是造成公众信息安全感的缺失。2018 年 12 月发布的《公共安全感蓝皮书：中国城市公共安全感调查报告（2018）》称，中国城市居民对信息安全感最低，信息安全感指数在全部城市公共安全感分项指标中倒数第一，这与电信诈骗的发案率密切相关。反言之，公众信息安全感可提升的空间较大，迫切需要加强对个人信息的保护。

2 信息泄露原因分析

敏感信息是指用户或企业单位所独有的不可公开的隐私信息，一般包括：个人信息、鉴别信息和商业信息三种。个人信息指的是用户身份的相关属性，如姓名、手机、身份证号、邮件等信息，在部分行业（如政府、金融行业）的系统中往往具有强实名信息。鉴别信息是指用户进入系统所使用的认证信息，如用户名、密码、动态口令等信息。商业信息是指用户在系统中的商业操作记录，如采购信息、竞价信息等。此三类信息一般均统一存储于信息系统的数据库中，是大部分信息泄露的总源头。但是这三类信息分别具有不同的用途，泄露后产生的风险也不尽相同，具体如表 1 所示。

表 1 敏感信息泄露风险情况

泄露源	影响程度	发生概率	泄露风险
个人信息	一般	高	遭受垃圾短信、邮件、推销电话的骚扰或受到非法分子的恶意欺诈，带来经济损失
鉴别信息	严重	中	可能导致账户中的金额被转移，发生未预期的转账或网络支付等操作
商业信息	危急	低	可能使企业蒙受巨大的经济损失（如竞价信息被竞争对手获取），还可能导致企业面临战略失败等重大变革

此外，在了解泄露源和泄露风险的情况后，还应深入分析敏感信息泄露的其他三个重要因素，分别为泄露原因、泄露方式和泄露渠道。敏感信息泄露的总体情况如图 1 所示。

目前大部分机构存在信息泄露的脆弱点。如有些互联网系统存在 SQL 注入、跨站脚本等漏洞，可能被恶意人员从互联网发起攻击，获取数据库权限导致信息泄露等。部分系统虽然为内部系统，但内部业务终端可访问互联网，一旦该终端受到病毒木马的攻击，则导致系统中的敏感信息遭泄露。

泄露的方式却有多种情况，一般分为内部泄露和外部泄露两种。外部泄露是指机构以外的人员利用系统漏洞通过互联网攻击或布置钓鱼网站欺骗用户等手段，获取用户的敏感信息。随着日愈猖獗的黑客盗取数据库行为，从 2011 年爆发 CSDN 的 600 万用户信息泄露，至相继而来的京东商城、美团网等电商沦陷，外部泄露危害的频繁度与严重性可见一斑。另一种为内部泄露，是指机构人员及外包

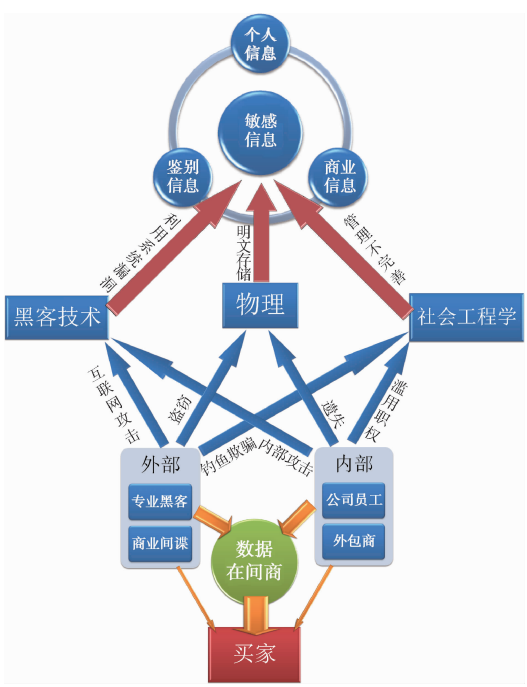

图 1 敏感信息泄露示意图

人员等能够接触内部系统的职工发生的信息泄露。国内70%的泄密事件均为内部泄密,这是由于内部人员拥有天然的合法权限访问信息数据。如果内部人员信息安全意识不高,可能遗失存有明文敏感信息的移动介质,造成大量信息泄密。又或者内部业务人员甚至是系统管理人员出于个人利益目的将用户敏感信息泄露给数据中间商,他们不仅可以将自己所拥有的系统权限范围内的信息泄露,还可以通过内部攻击系统,得到更多的用户敏感信息,这类攻击容易得手是由于系统往往对内防护较弱而导致的。另外,有些机构对系统的开发或运维采取外包的方式,且对赋予外包商较大的权限去访问系统,使得外包商可接触到系统内的敏感信息,一旦外包商的管理不完善也会造成大量敏感信息的泄露。敏感信息泄露的渠道一般为:第一手由外部黑客或内部人员非法获取、转至数据中间商、最终到达买家。泄露渠道每个环节的相关情况如表2所示。

表2 敏感信息泄露渠道情况

环节	具体情况描述
卖家	外部黑客或内部人员主动将非法手段获取的敏感数据倒卖给数据中间商。直接将数据提供给买家的情况较少
数据中间商	数据中间商将信息买卖发展至长期的“产业链”,大量的数据买卖平台打着数据交流的名头存在,已有职业化的趋势
买家	一般为广告商或销售公司,利用“精准广告”、“调查取证”的灰色地区,实施精准欺诈等犯罪行为

3 个人信息保护解决措施

个人信息保护是个庞大的系统性工程,做到真正防护要做到三个“不”,即“拿不到”、“用不了”、“逃不掉”。“拿不到”是指恶意人员无法通过非正常手段获取大规模的个人信息;“用不了”是指恶意人员对已拿到的个人信息无法进行非法使用;“逃不掉”是指恶意人员进行个人信息的违法使用后将受到法律的制裁。

3.1 加强信息安全防护

监管部门加强整体监督,政府部门建立基础保障平台,企业采取全面防护措施以及用户提高信息保护意识。

(1)监管部门加强整体监督应积极开展信息盗取的专项研究,对机构采取合规支撑、培训认证、技术检查的方法指导其尽量避免发生敏感信息泄露事件。合规支撑是个人信息保护的制高点,监管部门可以根据国家法律法规加强监督,根据不同的业务条线对所管辖的机构进行特殊规范,通过专项个人信息保护的研究,明确业务开展范围。健全企业自查汇报机制、群众举报机制以及风险共享机制。培训认证是为了唤醒与提高机构和用户对信息安全,尤其是敏感信息保护的意识,明确信息管理的重要性。监管部门可联合行业协会等单位共同举办相关的培训,开展相关考试和认证。技术检查是一种强制监督手段,进行定期检查。具体方式可针对信息系统的脆弱点作一个深入的检查,如敏感信息分类、加密存储与传输、敏感信息访问控制、非授权复制等,深入挖掘信息泄密重要的脆弱点,同时也针对整个信息系统的业务逻辑进行排查,基于业务流程的方法判断系统存在的逻辑漏洞及相关风险,有效保障敏感信息在业务处理过程中能得到一定的隐匿与保护。

(2)政府部门首先可通过引入新技术新应用的方式,提供全新的基础保障平台。在生物识别方面,由于个人生物信息(如人脸、指纹、虹膜等)的不可更改性,一旦泄露可能导致无法弥补的后果。故可建立统一的个人生物信息特征库。当企业需要个人信息进行比对时,只能统一通过向政府购买服务的方式,才能完成生物特征值的比对,而不能通过私自收集个人生物信息完成识别。再如区块链技术的应用,可利用区块链的特性(如保密性、可追溯性等)将个人信息控制权重新交回到用户。基于区块链技术普通个人能够在建立数字身份的同时亲身参与实现个人信息的保护,自行控制是否允许特定组织或个人访问、储存、分析或分享自己个人信息。

其次,可采用可信环境思想,采用可信计算、可信网络等技术实现个人信息保护,如目前广泛采用的手机TEE方式,能够有效保障个人信息存储在一个安全可靠的环境中。同时打造一个拥有可信用户、可信网络、可信终端、可信业务系统平台等各方面安全可靠的整体可信网络体系。

最后,政府部门还可将个人信息保护作为对各单位的重要绩效考核指标之一,提高单位领导对于个人信息保护的重视程度,以加强各方面管理要求

和技术要求的落实,提高单位整体的个人信息安全保护意识。

(3)企业采取全面防护措施应从两方面入手。第一,在技术上经常对系统各层面的漏洞进行检测,并及时进行安全补丁更新,尽可能地杜绝来自外部的攻击。此外,部署有效的安全防护设备、行为审计设备等,时刻关注来自外部和内部的异常行为。对于重要的敏感信息应该使用符合国家密码管理规定的密码技术进行加密存储,以提高整体的防护力度。第二,在管理上建立完善的审计与制约机制,对内部人员的权限实现最小分配,并设置安全管理员、审计员等重要角色,实时监控内部人员的非法操作。同时制定严格的管理制度,对泄露内部资料的人员以实施严厉的惩罚措施。此外,对于外包服务商则需采取严格的审核措施,尽量避免其接触到客户的个人敏感信息。

用户提高信息保护意识是关键的一环,因为个人数据采集的源头在于用户,让用户了解个人信息的价值、泄露方式、泄露危害等,才能有效提高用户的个人信息防护意识,在源头上将信息泄露的风险降到最低。

3.2 建立可信社会体系

实现"用不了"是我国建成可信社会体系的重要体现。违法人员即使拿到大量的个人信息也无处可使,再多的个人信息也只是烫手的山芋,量刑的证据。所以要做到这点需要运营系统对个人信息做到严格限制和政府采取全面征信体制。

(1)运营系统对个人信息的使用进行严格限制。个人信息被违法人员盗取后,主要通过通信方式进行利用,一般为打电话、发短信、发电子邮件等。而这些动作都需要依靠运营商进行。运营商可以通过目前的先进技术对非法使用个人信息的电话号码进行甄别、限制和禁用。如检测出单个电话号码每日发送的短信数远超出正常社交范围,且该电话号码不是企业备案的号码,就可对内容进行判断,若存在个人信息滥用的情况则可采取限制,严重时进行禁用,同时将这些黑名单或征信信息报送公共征信平台。

(2)政府采取全面征信体制。建议政府推进信用信息基础平台的建设,对于个人信息的违法利用,主要通过运营商的风控手段进行甄别。同时整合互联网络、政府征信资源(如工商、税务、法院、认证认可等)等数据信息,与公安、人民银行等权威征信系统进行对接和数据共享,建设政府的征信平台,提供统一、权威、可信的征信服务。

3.3 建立追溯机制

"逃不掉"是三个"不"中最后一环,是一种强烈的威慑力量。做到这一点需要法律明确惩戒立法保护个人信息,运营服务商进行实名验证以及公安机关加大打击力度。

(1)法律明确惩戒立法保护个人信息。建议对现有与个人信息保护相关的法律法规进行梳理,明确个人信息保护主体的责任与行为规范,并切实强化执行。另一方面,修订现有法律体系中与个人信息保护冲突的条款,在各个行业完善信息犯罪、责任追究的法律规范,补充制定在不同领域有利于个人信息保护健康发展的相关法规。

(2)运营服务商进行实名验证。在追查个人信息利用事件的调查方面,通信运营服务商起到至关重要的作用。在发生个人信息被大量利用的事件后,运营服务商应在事件发生后,利用自身业务的实名登记情况,查出使用者的相关信息并提交公安机关。对于存在不少恶意人员通过真实身份证办理电话卡的情况,运营服务商可以定期对非实名制用户或弱实名用户做到不断清理,建立可疑名单进行实时监控,一旦发现其发送违法信息后立即封锁,以加强实名制的真实性和有效性。

(3)公安机关加大打击力度。建议公安机关在收集到其他各部门提供的各类信息后,在个人信息侵犯的案件上加大办案成本,及时按照相关法律法规对黑产链条上的相关人员进行抓捕,并给予严厉处罚,特别是针对大量个人信息泄露的特大事件要严惩不贷,坚决打击各种类型的网络犯罪,形成对个人信息安全犯罪的高压打击态势,并逐步转变常态化模式。使盗窃个人信息的违法人员无处可逃,使觊觎个人信息的观望者退缩放弃,使企业和用户从意识上提高警觉,更加重视维护自身的信息安全。

4 结论

综上,个人信息安全不同于普通机构的网络安全,其泄露的影响涉及面较广,危害具有长期性,必须投入更大的成本进行保护。我国在信息技术快速发展的同时,需要充分认清面临的个人信息泄露风险,需要政府、行业主管部门、企业、测评机构、信息安全服务提供商用户等多部门、(下转第 33 页)

装备制造技术,2018(6):101-104.
[2] 钱锦锋. 逆向工程中的点云处理[D]. 杭州:浙江大学,2005.
[3] 柯映林,范树迁. 基于点云的边界特征直接提取技术[J]. 机械工程学报,2004,40(9):116-120.
[4] 王晓辉,吴禄慎,陈华伟. 基于区域聚类分割的点云特征线提取[J]. 光学学报,2018,38(11):58-67.
[5] 李羿辰,耿国华,张雨禾,等. 基于区域扩张的三维点云模型配准算法[J]. 计算机工程,2017,43(11):204-209.
[6] 王婉佳. 点云特征提取与拼接算法研究[D]. 哈尔滨:哈尔滨工程大学,2018.
[7] 周建钊,颜雨吉. 逆向工程中点云特征提取技术研究[J]. 装备制造技术,2019(8):13-17,33.
[8] 史皓良. 三维点云数据的去噪和特征提取算法研究[D]. 南昌:南昌大学,2017.
[9] 贺彤. 点云的特征线提取算法研究及应用[D]. 太原:中北大学,2018.
[10] DEMANTKE J,MALLET C,DAVID N,et al. Dimensionality based scale selection in 3D lidar point clouds [J]. ISPRS - International Archives of the Photogrammetry, Remote Sensing Spatial Information Sciences, 2011, 3812(5):97-102.
[11] 宣伟,花向红,邹进贵,等. 自适应最优邻域尺寸选择的点云法向量估计方法[J]. 测绘科学,2019(6):101-108.
[12] WEINMANN M,JUTZI B,MALLET C. Semantic 3D scene interpretation: a framework combining optimal neighborhood size selection with relevant features [J]. ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences,2014(II-3):181-188.
[13] 程效军,贾东峰,程小龙. 海量点云数据处理理论与技术[M]. 上海:同济大学出版社,2014.
[14] 朱德海,郭浩,苏伟. 点云库 PCL 学习教程[M]. 北京:北京航空航天大学出版社,2012.

(收稿日期:2019-12-18)

作者简介:

周建钊(1965 -),男,博士,教授,主要研究方向:机械设计及理论。

颜雨吉(1994 -),通信作者,男,硕士研究生,主要研究方向:机械装备三维建模与数字化技术。E-mail:yanyujis@126.com。

陈晨(1997 -),男,硕士研究生,主要研究方向:机械装备三维建模与数字化技术。

(上接第 22 页)

跨领域、跨行业的多方位合作才能够给予个人信息较好的安全保障。

参考文献

[1] 中华人民共和国. 网络安全法[Z]. 2017-06-01.
[2] 国家互联网信息办公室. 数据安全管理办法(征求意见稿)[Z]. 2019-05-28.
[3] 中央网信办,工业和信息化部,公安部,市场监管总局. 关于开展 App 违法违规收集使用个人信息专项治理的公告[Z]. 2019-01-25.

(收稿日期:2019-12-05)

作者简介:

倪惠康(1985 -),男,硕士研究生,高级工程师,主要研究方向:网络安全测评、个人信息保护。

何菲(1984 -),女,硕士研究生,工程师,主要研究方向:高校网络安全、等级保护测评、安全运维。

版权声明