科技民生报告丛书

大数据时代的隐私保护

中国科协学会服务中心　主编
中国通信学会　编著

中国科学技术出版社
·北　京·

图书在版编目（CIP）数据

大数据时代的隐私保护 / 中国科协学会服务中心主编；中国通信学会编著 . — 北京 : 中国科学技术出版社 , 2019.1

（科技民生报告丛书）

ISBN 978-7-5046-8224-6

Ⅰ. ①大… Ⅱ. ①中… ②中… Ⅲ. ①数据处理—安全技术 Ⅳ. ①TP274

中国版本图书馆 CIP 数据核字（2019）第 016552 号

责任编辑	夏凤金
装帧设计	中文天地
责任校对	梁军霞
责任印制	李晓霖

出　　版	中国科学技术出版社
发　　行	中国科学技术出版社发行部
地　　址	北京市海淀区中关村南大街16号
邮　　编	100081
发行电话	010-63583170
联系电话	010-63582180
网　　址	http://www.cspbooks.com.cn

开　　本	720mm × 1000mm　1/16
字　　数	121千字
印　　张	9
版　　次	2019年1月第1版
印　　次	2019年1月第1次印刷
印　　刷	北京博海升彩色印刷有限公司
书　　号	ISBN 978-7-5046-8224-6 / TP·410
定　　价	42.00 元

丛书策划组

总 策 划　宋　军

策　　划　申金升　朱文辉

执　　行　陈　光　张海波　刘　欣　唐思勤

本书编委会

首席专家　邬江兴

主　　编　陈玉玲　雷　敏　杨义先

编　　委（排名不分先后）

郭玉翠　康海燕　罗　群　陆天波　任　伟

尚　涛　叶　敏　张延川　张海君　章嘉懿

编 写 组　杨　榆　钮心忻

丛书序

科技工作永葆初心　人民生活赖之以好

习近平总书记在十九大报告中指出，中国共产党人的初心和使命，就是为中国人民谋幸福，为中华民族谋复兴。“靡不有初，鲜克有终”。实现中华民族伟大复兴，需要一代又一代人为之努力。初心和使命正是激励人们不断前进、不断取得事业成功的根本动力。总书记在“科技三会”上提出，“科技是国之利器，国家赖之以强，企业赖之以赢，人民生活赖之以好。中国要强，中国人民生活要好，必须有强大科技。”这不仅是新时代对科技工作提出的要求，更是广大科技工作者投身科技事业的初心。

作为科技工作者的群众组织，中国科协自 1958 年正式成立以来，在近六十年的发展历程中，一直将人民群众的需求、参与和支持作为事业发展的基础。科技事业是人民的事业，人民群众的支持就是科协事业发展的根本动力，人民群众的需求就是科协工作的主要方向，人民群众的参与就是科协工作的坚实基础。在党中央、国务院的正确领导下，中国科协不断健全组织、壮大队伍，通过各级学会和科协各级组织团结带领广大科技工作者围绕中心、服务大局，在推动改革开放、实施科教兴国战略和人才强国战略、建设创新型国家方面做出了应有的贡献。

当前，中国特色社会主义已进入了新时代。随着经济社会不断发展，我国社会主要矛盾已经转化为人民日益增长的美好生活需要和不平衡不充分的发展之间的矛盾，这对科技工作提出了新任务新要求，需要科技创新在推动解决发展不平衡不充分方面发挥更大作用，提高社会发展水平，改

善人民生活，提高全民科学素养。科技工作者更要积极行动起来，认清新时代新变化新任务新使命：让科技更好惠及民生、创造人民美好生活。科技的发展承载着 13 亿多中国人民对美好生活的憧憬和向往。科学研究既要追求知识和真理，也要服务于经济社会发展和广大人民群众，要想人民之所想、急人民之所急，将人民的需要和呼唤作为科技工作的动力和方向。为人民创造美好生活，必须牢牢抓住并下大力气解决人民最关心最直接最现实的问题，必须多谋民生之利、多解民生之忧，必须始终把人民利益摆在至高无上的地位，让科技发展成果更多更彻底惠及全体人民。

为深入贯彻党的十九大精神和习近平总书记在“科技三会”上的重要讲话精神，中国科协学会服务中心组织动员中国科协所属全国学会、协会、研究会，发挥科技社团专家的群体智慧和专业优势，编撰出版了《科技民生报告》系列丛书。这套丛书针对广大社会公众关切的热点和焦点问题，发出科技界的最新认识和回应，让科学知识走进千家万户，让科技成果服务广大公众。在编写过程中，我们深深感觉到，科技不是万能的，限于科技发展的客观水平，当前很多民生关切问题，科学技术还不能提供完美的解决方案。所以，这套丛书出版，不仅是向公众展示科技界已经取得的成绩，更是科技界继续奋斗解决民众关注问题的一份誓言书。我们希望能够不断满足人民日益增长的美好生活需要，使人民获得感、幸福感、安全感更加充实，更有保障，更可持续。

中国科协学会服务中心

2017 年 12 月

再序

关注新时代的科技民生热点

2018 年是改革开放 40 周年和中国科协成立 60 周年，中国科协正以崭新面貌昂扬走进新时代。新时代新征程对科技创新的战略需求前所未有，党和国家的事业对广大科技工作者提出的殷切期望前所未有，党中央对科协工作的关心重视前所未有。中国科协以习近平新时代中国特色社会主义思想为指导，深入落实中央群团工作会议、“科技三会”和中央经济工作会议精神，以智库、学术、科普为重点，以国际化、信息化、协同化为导向，把厚植党执政的群众基础作为首要政治责任，推动各学科领域的最新进展面向社会公众及时传播，帮助公众了解科学进展，激发科学热情，让更多的科技工作者和人民群众对科技发展享有更深切的获得感。

今年是《科技民生报告丛书》出版的第二年。在丛书第一辑取得了良好社会反响的基础上，为更好贯彻落实中国科协书记处关于智库、学术、科普三轮驱动、推动工作格局重塑的要求，学会服务中心将科技民生报告列入学会科技类公共服务品牌重点工作，组织专家和全国学会遴选主题、撰写编研，以专家视角、学术理性、科学观点，回应与人民息息相关的社会热点问题。通过专家观点引导社会公众树立理性认知，为科学决策提供意见建议，同时，服务科技工作者实现自身价值、获得社会认可、履行社会职责，更加充分发挥科学家的时代使命感、社会责任感。

《科技民生报告丛书》第二辑按照高站位、高标准、高质量的要求，更加注重丛书的品牌效应，贯彻创新、协调、绿色、开放、共享五大发展

理念，在内容设置上兼顾了学术、科普和咨询三大特色。一是立足学术，坚持科学性，由全国学会组织权威专家撰写，具有一定的学术价值；二是通俗易懂，体现科普性，以尽可能直白的语言让科学知识更多惠及基层群众，提升公民科学素质；三是适当前瞻，具备咨询特色，可为有关部门科学决策提供意见和建议。

希望本套凝聚科技工作者智慧的丛书，能在弘扬科学精神、普及科学知识、普惠科技成果、倡导创新文化方面发挥一点积极的作用，激励广大科技工作者不忘初心、牢记使命，在新时代抓住机遇、乘势而上，焕发新气象，实现新作为，为建设美丽中国、健康中国、智慧中国、构建人类命运共同体做出更大贡献。

中国科协学会服务中心

2018 年 11 月

本书序

与传统意义的隐私数据相比，大数据时代下的隐私数据范围更广，导致一些不法分子开始大肆获取大数据中包含的个人隐私数据，以牟取不义之财。一旦个人的隐私信息被泄露，给信息所有者不仅可能带来经济损失，还可能带来名誉损失等难以挽回的影响，甚至造成人身伤害。一连串在社会上引起轰动的网络隐私数据外泄事件给人们敲响了警钟，个人信息尤其是隐私数据的保护非常重要。

大数据时代下用户隐私数据保护是重要的研究课题，广大科技工作者为此付出了大量心血，并取得很多新进展。但是，隐私数据保护不仅依赖科研人员的努力，还需要人们了解隐私保护的相关知识，从自身做起，从源头减少隐私数据的泄露。法律界需要制定严格的个人隐私数据保护的法律法规，相关企业应加强安全建设，在使用用户数据的同时也应担负起社会重任，以保护隐私数据。同时，我们要凝聚多方力量形成合力，共同推动大数据隐私保护，通过科普图书宣传提高全民的防范意识是非常重要的手段之一。

本书旨在以问题为导向，回应公众关切的问题，从而宣传个人隐私数据保护的重要意义，促进对个人数据的合法安全使用。全书以独特的科普语言和图文并茂的方式，结合具体案例剖析大数据时代下个人隐私数据泄

露途径和后果，介绍隐私数据保护的相关知识，特别是一些实用的技巧，帮助普通大众保护个人隐私数据。

中国工程院院士　邬江兴

2018 年 9 月

前言

今天，最懂我们的似乎是互联网。电商网站了解你的消费喜好，专车平台清楚你每天的行踪，移动支付平台掌握你的财产变动……在大数据时代，我们的位置、通信、征信、交易等各类数据信息被源源不断地收集、存储在网络空间，每个人似乎都成了“透明人”。随着近几年网络隐私数据泄露事件的增多，人们不禁担忧，我的隐私数据是怎么泄露的？我该怎么保护我的个人隐私数据呢？这些疑问，相信在你读过本书后，都能得到解答。

科技民生报告项目由中国科协总体策划，中国科协学会服务中心组织实施。作为中国科协《科技民生报告丛书》之一，本书从人们关心的热点事件出发，结合典型案例，用生动有趣的语言，通过六个问题向人们讲述了大数据时代下不一样的隐私数据问题。本书在第一章“大数据技术对隐私保护有什么影响”，分析了大数据技术发展给人们生活带来的便利，并引出大数据技术带给隐私数据的威胁。第二章“什么是大数据时代的隐私权”中，回顾了隐私和隐私权的发展历程，并介绍由于观念改变和大数据技术发展带来的隐私含义的新改变。第三章“隐私泄露有什么后果”中，详细分析了隐私数据泄露后造成的影响，引起人们对隐私问题的重视。第四章“隐私是怎么泄露的呢”，从个人无意识泄露、倒卖数据窃取、入侵手机、病毒入侵、网站漏洞五个方面，结合案例详细介绍了隐私泄露的途径。第五章“大数据时代下如何保护个人隐私”，从人们自身、科学技术、

行业社会以及国家立法四个角度，为人们介绍了保护隐私数据的方法，消除人们的担忧心理。第六章“未来如何保护隐私”，立足于未来，从政策和技术角度，探索讨论如何在大数据动态发展下进行隐私保护。

信息社会下，数据成了最宝贵的资源之一。政府利用大数据技术为人们生活提供便利，建设智慧城市，企业利用大数据技术分析潜在的顾客群体，判断未来的发展走向，如果仅仅因为隐私数据泄露问题放弃大数据技术的应用，这无疑是因噎废食，因此如何保证大数据时代下的隐私数据安全成了人们和社会重点关心的问题。为了解决民众的担忧，推动大数据更好地发展，国家积极出台各项法律法规和行业规范，规范使用用户隐私数据的行为，广大科研人员也付出了大量心血，在大数据应用中每个可能泄露隐私数据的阶段，都不遗余力地研究对应的技术保护方法。本书作为一本科学性的普通读物，只是浅显地介绍了大数据技术造成隐私数据泄露的可能性，帮助人们认识到保护隐私数据的重要性，书中难免存在疏漏和不妥之处，恳请各位同行专家和各界读者批评指正。

科学普及是中国通信学会的主要任务之一，是学会深入贯彻《全民科学素质行动计划纲要（2006—2010—2020 年）》的重要工作。在本书编写过程中，中国科协学会服务中心给予学会大力支持和帮助，中国通信学会张延川秘书长、薄旸老师积极协调，编委会专家及北京邮电大学和贵州大学等编写组的老师们秉承科学的严谨态度，投入了大量时间和心血，在此一并表示感谢！

目录 Contents

第一章
大数据技术对隐私保护有什么影响？ / 001

第一节 大数据让生活更美好 / 002
第二节 大数据带来隐私安全挑战 / 009
第三节 2017 年十大信息泄露安全事件 / 013

第二章
什么是大数据时代的隐私权？ / 019

第一节 隐私权的发展 / 020
第二节 大数据时代的隐私特征 / 022
第三节 大数据时代的隐私权 / 026

第三章
隐私泄露有什么后果？ / 029

第一节 隐私泄露无处不在 / 030
第二节 隐私保护新挑战 / 035
第三节 隐私泄露影响广泛 / 039

第四章
隐私是怎么泄露的呢？ / 043

第一节 个人泄露 / 044
第二节 数据窃取 / 049
第三节 公共设备漏洞 / 059
第四节 恶意程序 / 065
第五节 网站漏洞 / 077

第五章
大数据时代下如何保护隐私？ / 081

第一节 个人主动保护 / 082
第二节 科技保护隐私 / 093
第三节 行业社会保护 / 101
第四节 国家法律与政策保护 / 104
第五节 国际隐私保护经验 / 109
第六节 隐私泄露后的补救措施 / 112

第六章
未来如何保护隐私？ / 117

第一节 人工智能打击黑产 / 119
第二节 网络态势感知 / 121

参考文献 / 127

第一章

大数据技术对隐私保护有什么影响？

第一节 大数据让生活更美好

大数据和人们日常生活中衣食住行的联系越来越紧密，为民众的生活带来了许多便利，让民众的生活方式在不知不觉间发生重大改变，人们可以更加轻松地获得想要的东西。

不用逛街逛到腿软也可以买到更合适、更称心的衣服，预约量体裁衣，在线选择款式工艺，工厂生产专属的数据板型，手机支付货款……这些在大数据技术没有出现以前，只存在于人们的幻想中。如今，以大数据为支撑的“互联网 + 私人定制”模式改变了传统制衣模式，利用大数据打破传统的制衣模式，把所有繁复传统的制衣过程变成了简单快捷的线上量体裁衣，将只依靠量体师量出来的人体尺寸变成了更准确更精密的人体大数据。最后再根据线上测量的数据制成成衣，这样每个人都可以成为自己的服装设计师。

民以食为天，大数据技术在餐饮行业的应用，让人们吃得更好、更方便。在互联网没有出现以前，朋友聚会找餐厅可能就是满大街的“瞎逛”，或者是熟人推荐，有了互联网以后，就是上网去搜索一些有名的、有人气的餐厅，但是对于餐厅的评价，甚至是具体的地理位置都可能摸不清。随着大数据技术的不断发展和深入，人们的餐饮以及消费方式也发生了翻天覆地的变化，外卖平台也迅速发展起来，为人们的生活带来便利，互联网上可以找到餐厅的位置、价格以及评价，极大地满足了人们的饮食需求。大数据还能让人们吃得更安全更放心，扫一下二维码就可以知道农产品是从哪里生产出来、产地环境如何等信息，甚至可以体验农产品在种养殖、加工、检测、流通、营销等环节一体化的数据服务。

大数据做出的精准判断可以让我们的出行变得更加美好，人们完全可以根据自己的需要随时随地呼叫用车，汽车将不再是每个家庭的生活必需品，人们也不必担心司机和停车问题，公共资源可以被最大限度地利用，同时释放出更多城市空间。

随着大数据技术的发展，智能化的综合网络将遍布社会各个角落，渗透我们的日常生活的每个角落，影响和改变的不仅是人们衣食住行的生活方式，还影响着人们的学习方式、工作方式和娱乐方式。总的来说，大数据在我们生活中的影响主要有以下方面：

1. 智慧城市

哪里交通拥堵、哪里人流量增多、哪里的空气质量不好……一座城市的关键治理数据可视化地展现在一块大屏幕上，大数据可视化系统平台可以涵盖智能交通、应急指挥、城市管理、公共安全、环境保护等领域，为城市管理与运行提供决策支持。

随着社会经济的发展，交通工具的种类和数量日益增多，给城市交通管理带来极大的不便和安全隐患，经常出现拥堵、资源应用不合理的情况。大数据在社会安全管理领域的应用极大改善了群众使用私家车的出行状况，通过对手机数据的挖掘，可以分析实时动态的流动人口的来源、出行，实时发布交通客流信息及拥堵情况，帮助人们合理规划路线，尽量避开交通拥堵路段，“晚高峰下班，连遇 20 个绿灯！”这不是你运气好，而是红绿灯会思考。大数据还可以通过分析预测出行交通规律，科学调整车辆派遣密度，进行车流指挥控制，及时做到疏理拥堵，减轻交通压力。此外，大数据也给使用公共交通、打车出行的人们带来极大的便利，以往很多人都有在寒冷或酷热的户外苦苦等公交车的经历，如今出门前只需要提前查询地图，就知道车辆多久能够到站。例如，北京交管部门通过将实时路况与百度地图大数据对接，依托百度地图的交通大数据，可为公众提供专业的城市实时交通信息，并可根据需要自行选择，满足个性化出行需

求，提升出行效率。

2. 医疗民生

与民生福祉密切相关的健康医疗领域也在逐步应用大数据。搜集患者临床医疗数据与体征数据，数字化病历档案，使得医生可以在民众个人医疗数据库的基础上进行远程诊疗和医疗研发，从而大大提高供给端的服务能力和效率，解决中国医疗领域存在的诸多问题，比如优质资源短缺、医疗费用高、医生工作强度大等痛点。除了疾病诊疗的准确度和效率大大提升，还有可能预测疾病的走势，通过及时调整将疾病的影响控制在最小范围，比如利用大数据技术预测流感、手足口病、肝炎、艾滋病、肺结核等主要传染病动态，预测未来的传染病趋势，以便及时调整医疗资源或者是实施预防手段。

3. 精准营销

企业通过大数据挖掘技术对用户的行为习惯和喜好进行追踪分析，将每个用户在其网站上的行为数据进行记录和分析，提高与用户的沟通效率、提升用户体验，实现了向不同用户展示不同内容的效果。比如，针对用户不同的属性特征、性格特点或行为习惯，在他们搜索或点击时，网站将展示符合该用户特点和偏好的商品，尽力给用户提供友好舒适的购买体验，有效提高用户的购买转化率甚至使其重复购买，提高用户忠诚度和用户黏性。这也是我们在网上购物，页面总能很“神奇”地出现我们最想购买的商品的原因。

讲到这里，有人可能会问，大数据技术真的有这么厉害吗？它真的可以颠覆我们的生活方式吗？通过分析大数据在医疗行业的应用，你会感到大数据技术在生活中的影响。

生病就医是关乎老百姓生活质量的民生大事。过去，患者的病历信息和住院信息都是通过手写的方式进行记录，我们为了获得准确的诊疗交出

我们的隐私数据，包括姓名、年龄、近期活动情况、既往病史、家族病史等，但手写的方式不仅使患者的就医程序极为烦琐，还在一定程度上提高了医院的管理成本。

大数据技术的出现推动了医疗行业的转型升级和创新，改变传统就医诊疗的方式，将患者就医的隐私数据全部转化为电子数据进行保存，使得医生通过智能终端查看患者情况成为可能（图 1-1）。比如医生可以打开随身携带的平板电脑，登录浏览当天住院患者、新入住患者的整体情况，点击其中一位患者的名字，可了解这个患者的姓名、床号、入院时间、主管医生等基本情况，据此可为患者提供量身打造的医疗保健，让医疗行业的发展更智慧。

图 1-1　大数据下的医疗数据

在医疗领域，大数据分析的作用不容小觑。数据平台记录人们的健康数据，包括人们的日常健康体征数据、体检数据、病例数据、处方数据、

用药情况数据、基因数据等围绕着人体各项健康指标以及与健康行为相关的数据，这些数据可以用来为我们建立电子健康档案、电子病历、电子处方等个人医疗数据库。大数据技术还可以将医学专家积累的宝贵经验转化成标准化的知识基础，在民众个人医疗数据库的基础上进行诊断、治疗，从而大大提高供给端的服务能力和效率，解决中国医疗领域存在的诸多问题，帮助覆盖民众全生命周期的预防、治疗、康复和健康管理的电子健康服务。

随着大数据技术在医疗行业的应用，国内有平台借助大数据技术，推出一款移动健康咨询 App，为用户配备一位线上私人医生，在确保医疗隐私数据不被泄露的情况下帮助用户建立电子健康档案，用户可以在线上咨询医生自己的身体状况或者上传自己的健康数据，比如测量的血压、心率，平台实时在线监测用户日常数据，并记录用户健康变化的数据。这样，不仅可以及时发现身体出现的疾病，在就诊时，医生看到的不只是用户一次疾病的情况，而是过往全部医疗数据的一个非常立体的展示。该平台目前已沉淀了千万量级的医患问答数据，主要集中在妇科、儿科、皮肤科等，用户在提出问题后，后台用大数据自动匹配类似的历史问题及相关症状的信息呈现给用户，给出诊断相似度比例由高到低排列的医生回复。这些属于隐私的医疗数据都被保存在加密的数据平台中，问题匹配的过程中也会对数据的所有者进行匿名化处理，用户的隐私信息得到保护。

除了对已有疾病进行诊断、处理，未来大数据技术还有可能对未发生的疾病进行预测（图 1-2）。通过积累的患者信息，搜集多个人的基因、多种体液、父母的遗传史信息，以及他们如何代谢食物、营养和药物，在压力下他们的心跳速度，化学反应如何改变他们的基因行为等，来全面描绘健康人的身体究竟应该是何模样，并利用大数据的分析能力发现疾病与人体生理特征的关系，从而帮助人们提前发现潜在的疾病。例如，人体可能存在一些有助于分解高脂肪食物的生物特征，拥有这些特征的人，可以将患上高胆固醇和心脏病的时间延后，没有这类特征的人则会更早患上心

脏病，一旦发现这一规律，平台便可以借助大数据匹配技术来发现那些缺乏这类特征的人，帮助他们纠正习惯，或者开发出新的疗法，减小这类疾病的发生概率。

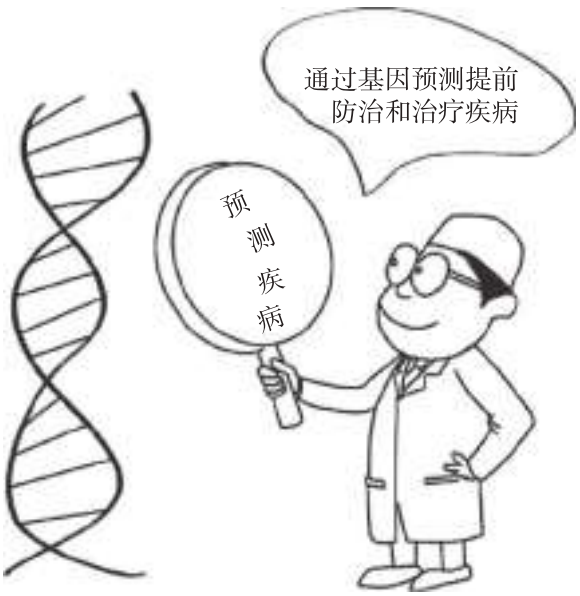

图 1-2　未来医疗大数据预测疾病

大数据在医疗中应用意义显而易见。

1. 节约时间

在大数据技术出现之前，患者就医需在医院大厅多次排队，无论是挂号、交费、排队候诊或者取报告等环节，而现在，在大数据技术的支持下，借助手机、电脑等互联网终端，去医院看病挂号、缴费不再需要排队。

2. 节约资源

通过大数据优化患者治疗方案，避免重复诊治。过去，患者在不同医

疗机构就医需要重复进行检查，不仅使患者就医程序极为烦琐，还在一定程度上造成医疗资源的浪费。医疗数据被数字化保存在平台上，通过大数据技术整合，可以让医生利用医院间互通的数据，结合患者具体的健康情况和既往病史，尽快做出诊断，而且让患者参与医疗全过程。保持医疗服务的连贯性和及时性，推动了医学研究、临床决策、疾病管理以及医疗卫生决策等方面的转变。

3. 个性化医疗

大数据技术在医疗服务上的应用提供了新的医疗模式，通过大数据统计推断或利用精准的生物医学数据获得患者特异疾病的通路，根据患者具体的身体情况，进行个性化的治疗方案设计，真正做到医疗服务的个性化和精准化，实现传统环境下难以完成之事。比如，每个患者的用药和治疗都不同，但由于传统情况下缺乏对于数据的采集和分析，信息严重缺失，患者的用药和治疗都“被标准化”了，这其实是不合理的，但是在大数据的支撑下，可以精准地给出用药指导，不再是“一次一片，或者一次几片”。

4. 减少疾病发生

大数据在医疗领域的应用为患者带来了许多的便利和改善，使得“上医治未病”成为可能。通过医疗数据分析，患者在身体从健康状态到亚健康状态的转变中，能够得到及时的提醒，并得到个性化、有针对性的指导建议，防患于未然。既减少了患者的病痛，又减轻了其经济压力。

未来，大数据将在社会治安、医疗、交通等各个领域全方位地改变我们的生活，未来的生活到底能有多智能，现在尚难以想象，这里借用大数据概念之父托夫勒的一句名言：“唯一可以确定的是，明天会使我们所有人大吃一惊”。

第二节　大数据带来隐私安全挑战

大数据技术是把双刃剑，虽然它给我们的生活带来了众多便利，但只要有数据，就必然存在安全与隐私的问题，各种因隐私泄露造成的案件也越来越多。中国互联网协会发布的《中国网民权益保护调查报告》显示，54% 的网民认为个人信息泄露严重，其中 21% 的网民认为非常严重，并且有 84% 的网民亲身感受到了由于个人信息泄露带来的不良影响。据统计，仅仅从 2015 下半年至 2016 上半年的一年时间里，个人信息泄露造成的总体经济损失达 915 亿元。

被肆意泄露的精准的个人信息成为电信诈骗的“先决条件”。上述报告中还显示：76% 的网民遇到过“冒充银行、互联网公司、电视台等进行中奖诈骗的网站”，66% 的网民曾经收到“冒充 10086、95533 等伪基站短信息”，55% 的网民收到过“冒充公安、卫生局、社保局等公众机构进行电话诈骗”的诈骗信息，51% 的网民收到过“冒充苹果、腾讯等公司进行钓鱼、盗取账号的电子邮件”，还有 47% 的网民遇到过在“社交软件上冒充亲朋好友进行诈骗”的情况，37% 的网民因收到上述各类诈骗信息而遭受到钱财损失。

电商平台给快递行业带来了前所未有的机遇，人们足不出户，就可以通过快递收到自己心仪的物品，这本是一件令人开心的事情，但是如果你用快递的个人信息被非法使用呢？前不久，圆通速递近百万条快递单个人信息在网络上被公开出售，网上甚至还出现了专门交易快递单号的网站，如“淘单 114”“淘铺发”“淘单网”“单号吧”等。在这些网站，每个单号都被明码标价，“批发价”最低四角，俨然已成为一种“产业”。据调

查，每天在网上交易的快递单号高达 3 万个左右。这些单号信息中有我们大量的敏感信息，比如姓名、电话、快递信息和地址等，尤其是在快递要求实名制认证后，我们使用快递服务时的身份证号也被收集。一旦掌握信息的服务商监管不到位或者不法分子想以此牟取利益，我们的个人敏感信息就可能被非法使用，给个人带来安全隐患。

除了快递行业中信息被明码标价贩卖外，其他行业的用户隐私信息泄露贩卖也相当猖獗，已经发展成为一条地下数据黑色产业链。国内知名信息安全团队“雨袭团”发布报告称，仅仅 2016 年，高达 8.6 亿条个人信息数据被明码标价售卖，有的还被卖过好几手，数据黑市之猖獗由此可见一斑。下面列举一组网络上贩卖隐私信息的报价表（表 1-1）：

表 1-1　隐私信息贩卖价格表

信息项目	价格	用途
身份证户籍信息	10~40 元 / 条	制作假通缉令、法院查封令，实施精准电信诈骗
		用他人身份注册网店，销售毒品等各类违禁物品和假冒伪劣产品
		冒名办理信用卡等进行恶意透支
		冒名在网贷平台进行恶意贷款
		冒名开办银行卡及第三方支付账号，接收和转移非法资金及洗黑钱
		冒名挂失他人手机号码，为实施诈骗等犯罪做准备
车辆信息	10~40 元 / 条	仿冒交通违章类电话短信实施诈骗
		发送车险等恶意推销广告

续表

信息项目	价格	用途
开房记录	150~500 元 / 次	私家侦探业务
		抓奸、查婚外情
		非法讨债
手机基站位置	200~500 元 / 次	私家侦探业务
		非法讨债
手机话单	2000~3000 元 / 次	私家侦探业务
		非法讨债
		商业间谍
银行开户资料	1~10 元 / 条	精准发送钓鱼或者木马链接，实施银行卡盗刷等诈骗
		冒充银行职工或者公检人员进行电信诈骗
		非法查询他人财产状况，为其犯罪做准备
银行流水单	1000~3000 元 / 份	私家侦探业务
		非法讨债
火车购票信息	100~200 元 / 次	私家侦探业务
		行踪调查
PS 手持身份证	150~200 元 / 张	冒用他人身份注册网店，或进行第三方支付平台账户实名认证
		申请 POS 机，用于转移非法资金及洗黑钱
PS 动态认证视频	1000~2000 元 / 个	冒用他人身份注册网店，或进行第三方支付平台实名认证
		对违规第三方账号进行解冻

续表

信息项目	价格	用途
PS 企业五证	800~1000 元 / 套	申请支付接口，用于转移非法资金及洗黑钱
		申请 POS 机，用于转移非法资金及洗黑钱
		冒用他人企业名义，进行恶意商业营销活动或诈骗
		开办虚假网站或钓鱼网站
		开网店、网贷等业务，销售假冒伪劣产品
		恶意贷款
PS 银行回执单	300 元 / 份	汇款转账类诈骗

无独有偶，用户隐私信息泄露的案件从来都不是个例，在圆通事件后不久，携程也随之出现大规模数据泄露，而且此次数据泄露无论是规模还是影响，都远远超过圆通速递，因为此次泄露的信息含有用户的银行卡信息，主要包括用户的姓名、身份证号码、银行卡类别、银行卡卡号、银行卡 CVV 码（即卡号、有效期和服务约束代码生成的 3 位或 4 位数字）以及银行卡 6 位 Bin（用于支付的 6 位数字）。那么这些信息为什么泄露呢？是因为网站在处理用户支付服务时，将部分持卡所有者向银行验证支付时的信息直接保存在本地，而这些支付敏感信息按照《银联卡收单机构账户信息安全管理标准》的规定，是不允许被各机构保存的，正是携程记录用户信用卡信息的“过度收集信息行为”，直接导致了此次信用卡隐私信息泄露危机。

大数据的发展正朝着全球化方向迈进，由大数据引发的隐私泄露侵权事件也出现了全球化趋势。Facebook 的 8700 多万用户数据泄露，是自创建以来最大的用户数据泄露事件之一，并且这些数据被“剑桥分析”公司非法利用以发送政治广告。剑桥分析公司与 Facebook 进行合作，剑桥

分析公司以有偿方式引导用户在 Facebook App（类似国内微信的小程序）上进行个性人格测试，不仅收集用户测试结果，还收集用户在 Facebook 上的个人信息，以此访问并获得了 8700 万活跃用户数据。这些被搜集的信息包括用户的住址、性别、种族、年龄、工作经历、教育背景、人际关系网络，平时参加何种活动，发表了什么帖子，阅读了什么帖子，对什么帖子点过赞等，可以通过这些数据刻画出详细的个人“心理画像”，并有针对性地投放广告。

近年来信息泄露事件呈现高速增长趋势，互联网行业是信息泄露的高发区，互联网企业应当更加重视数据安全以及用户个人信息保护，一旦发生泄露事件，对用户及企业都会造成严重损失。如果你还没有认识到个人隐私信息泄露就发生在你我身边，第 3 节中列举了 2017 年十大信息泄露的安全事件，一起来看看吧！

第三节　2017 年十大信息泄露安全事件

1. 辽宁破获特大侵犯公民个人信息案 百亿条公民信息泄露

2017 年 6 月 26 日，在公安部统一指挥调度下，辽宁省丹东市警方在北京、广东、湖南等地公安机关的协助下，对“4.26”特大侵犯公民个人信息案开展集中收网行动，捣毁 5 个通过互联网非法获取、贩卖公民个人信息并利用公民个人信息复制、盗刷银行卡的团伙。共抓获犯罪嫌疑人 31 名，查获涉及交通、物流、医疗、社交、银行等各类被窃公民个人信

息 100 余亿条。

据了解，这些诈骗团伙分工明确，组织结构严密，团伙与团伙之间经常有信息方面的交流。专案组民警介绍说，团伙除涉嫌公民信息犯罪外，还涉及非法侵入计算机系统犯罪和盗刷银行卡犯罪。其手中的原始公民信息数据一部分是通过链接在某网站上下载所得，另一部分是通过某破解软件在一些互联网网站下载所得。

2. 50 亿条公民信息泄露，京东前员工牵涉其中

公安部组织安徽、北京、辽宁、河南等地公安机关开展“9.27”特大盗窃贩卖公民个人信息案集中收网行动，抓获犯罪嫌疑人 96 名，初步查获涉及物流、医疗、社交、银行等各类被盗公民个人信息 50 亿条。

这起由公安部破获的盗卖公民信息特大案件中，犯罪团伙涉嫌侵略社交、游戏、视频直播、医疗等各类公司的服务器，非法利用公民个人信息精准推广网络游戏、网络赌博产品获利，还非法获取用户账号、密码、身份证、电话号码、物流地址等重要信息，并将这些信息出售给从事“黑产”的其他不法人员，从中牟利。另外，他们还在不断扩充所掌握的数据库资源，为攻击其他互联网公司提供支撑。其中犯罪嫌疑人郑某鹏在国内多家知名互联网公司工作，其长期与盗卖个人信息的犯罪团队合作，将从所供职公司盗取的个人信息数据进行交换，并通过各种方式在互联网上贩卖。

3. 5000 万优步（Uber）客户个人信息泄露

这一数据泄露事件实际上发生在 2016 年，但由于 Uber 公司的刻意隐瞒，大众直到 2017 年 11 月才知道这件事。已泄露的数据包括 5000 万名优步客户的姓名、电子邮件地址和电话号码。大约 700 万名司机的个人资料也被曝光，其中包括大约 60 万个驾照号码。

黑客首先访问了 Uber 工程师使用的一个私人 GitHub 网站，从而成

功地窃取了数据。从那里，他们获得了 Uber 的 AMS（亚马逊云计算平台服务）登录凭据，并访问了个人数据。用户个人隐私信息泄露在互联网中，无异于在大街上“裸奔”，用户的隐私权遭到威胁，个人信息安全无法保证，可能会收到来自四面八方的骚扰短信、邮件和诈骗电话。而司机驾照信息被泄露，可能导致车辆被非法追踪，威胁司机和乘客的人身安全。

4. 中国多家互联网巨头 10 亿条数据被抛售

暗网市场知名供应商“双旗”抛售从数家中国互联网巨头盗取的大量数据，数据条数达到 10 亿以上。这些数据来源于网易及其下属的 126.com、163.com 和 Yeah.net；拥有 QQ.com 的腾讯控股；TOM 集团的 Tom.com、163.net；新浪集团的 Sina.com/Sina.com.cn；搜狐公司的 Sohu.com；以及信网信息技术有限公司的 eYou.com。

这些数据来自多家互联网巨头公司，其用户群体广大，但是在隐私数据保密方面有所欠缺，被盗数据有些是很容易就能破解的密文，有些甚至是明文呈现。更让人心惊的是，因为“双旗”没有回应数据来源请求，公司对这些数据是怎么被泄露的都不得而知，给用户造成了极大的心理恐慌。

5. Equifax 1.43 亿信用卡信息泄露

美国最大的个人信用评估机构之一的 Equifax 在 2017 年 9 月 7 日发表声明称，由于遭遇黑客攻击，网络犯罪分子已经渗透到他们的网络中，泄露的信息包括社保号、生日、信用卡号、用户姓名、地址，甚至包括驾照号码，更糟糕的是，约 20.9 万名消费者的信用卡号码和 1.82 万人的信用报告纠纷相关文件也被曝光。

此次数据泄露规模涉及了 1.43 亿美国人的信息，根据美国统计局数据显示，美国目前总人口数约 3.2 亿，这意味着将近一半的美国人处在重

要隐私信息被泄露的风险中。该公司称，此次数据泄露事件是因为没打上2017年3月的一个安全漏洞补丁。

6. HBO再遭遇泄密！黑客盗取了1.5TB数据

2017年8月，全世界著名的美国娱乐业巨头HBO公司受到了黑客组织的攻击，被盗取了1.5TB的数据。黑客已在网上公布了《球手》和《104号房间》的未播出剧集剧本，此外还有尚未完整播出的《权力的游戏》等热门剧集、剧本，被盗取的信息中甚至还包括HBO核心网络构架信息、高管私人信息的文件。

HBO公司的信息安全危机不仅来自外部的黑客攻击，更是由于自身的问题导致“内忧外患”。影视作品从制到播的过程中，经手的公司多，环节也多，因此安全性受到挑战的风险尤其高。这次信息泄露事件不仅对公司造成了巨大的经济损失，公司的声誉也因此受影响，黑客甚至公然宣称“可怜的HBO再也无法崛起”。

7. 2亿美国选民资料被Deep Root Analytics泄露

数据分析公司Deep Root Analytics是由共和党全国委员会承包的，2017年6月，它泄露了超过1.98亿名美国公民的政治数据，这意味着每三个美国人中就有两个受到影响。被泄露的信息包括姓名、生日、电话号码，以及最令人不安的选民登记细节。

数据泄露的漏洞是由安全研究员Chris Vickery在6月12日发现的。他发现该公司的数据库存储在亚马逊的云服务器上，没有密码保护，时间大约持续有两周，在这期间，任何人都有能力下载这1.1TB的数据，引起了重大的隐私问题。

8. 58同城全国简历数据遭泄露

2017年3月，58同城全国简历数据遭泄露，网上有电商出售“58同

城简历数据”，并明言“一次购买 2 万份以上，3 毛一条；10 万以上，2 毛一条。要多少有多少，全国同步实时更新。”还有商家出售采集数据的软件，700 元一套。支付 700 元购买软件之后，可以用卖家提供的账号登录软件，在检索选项中选择北京市、所有职业、2017 年 1 月后更新过简历的活跃求职者，该软件开始不断采集信息，并且将所采集信息按照“姓名、手机号、求职方向、年龄、期望月薪、工作经验、居住地、学历、用户 ID、更新简历时间”等格式自动录入到 excel 表格中。在检索选项中，包括全国 430 多个城市以及 464 个职业选项。该登录账号有效期为 1 个月，如果需要不断获取 58 简历最新数据，每个月都需要续费 700 元。

如此庞大且实时更新的隐私数据曝光在互联网上，令求职者在投递简历的过程中提心吊胆。网络上，招聘网站允许企业、个人账号来搜索简历的同时，也为爬虫软件提供了可以采集简历信息的便利入口。而简历隐私信息的泄露不仅仅是因为外部的网络攻击，公司内部对信息的保护也并不严格，一位曾在招聘网站工作的人士透露，新来的实习生也可以跟主管要账号，登录数据库将求职者简历下载到个人电脑上，并且想下多少都可以，完全没有限制。

9. Xbox 和 PlayStation 盗版论坛 250 万账号被窃

Xbox360ISO.com 和 PSPISO.com 是两个 Xbox 和 PlayStation 盗版游戏的论坛。2017 年 1 月有国外媒体披露，在 2015 年年底，这两家网站遭到了匿名黑客攻击，导致 250 万用户账号被泄露。截至 2017 年 2 月 3 日，网站显示约有 129.7 万个 Xbox 360 ISO 账号和 127.4 万个 PSP ISO 账号被黑客入侵。

据外媒披露，这两家网站用户信息的保护措施并不完善，所有密码只是使用了 MD5 哈希系统进行加密，而这种防护方式非常容易被攻克，泄露的用户信息包括电子邮件、IP 地址、网站用户名称和密码。

10. 互联网连接泰迪熊泄露数以百万计的语音信息和密码

2017 年 2 月，有网络安全研究员提供一份调查报告，报告中表明，在短短两周内，“云宠物”（CloudPets）品牌超过 82 万个用户的账户信息被泄露，其中包括 220 万条语音信息。

“云宠物”品牌的泰迪熊是一款可以连接网络的智能玩具。这些玩具有一个功能就是允许儿童和亲属之间收发语音信息，并且该制造商将用户数据和语音数据储存在开放式的数据库中，这意味着任何人都可以不需要身份验证和密码就可以直接访问云端中储存的数据，最终导致这些音频数据和用户的私人信息成为了入侵者的目标，一同丢失的还有大量用户配置文件图片、儿童姓名和他们父母、亲人和朋友的部分信息，包括用户姓名、地址、电子邮箱及密码。网络上甚至已经出现对“云宠物”用户进行敲诈勒索的事件，要求用户交钱才能赎回信息文件，给用户的信息安全、财产安全甚至是人身安全造成了极大的安全威胁。

在如此严峻的网络安全环境下，人们对于隐私信息保护的需求越来越急切。在接下来的章节中，我们将从什么是大数据时代的隐私权，隐私泄露有什么后果，隐私是怎么泄露的，大数据时代如何保护隐私权以及未来如何保护隐私权这五个方面简要介绍大数据时代的隐私保护，帮助读者了解大数据时代下的隐私挑战并培养隐私安全意识。

第二章

什么是大数据时代的隐私权？

李彦宏说过，中国人愿意用隐私换方便。但是隐私并不是可以交换的，因为它是我们的一项基本权利！随着技术的发展，大数据带给我们的便利越来越多，随之而来的信息搜集也越来越多，隐私信息的边界不断模糊化，我们对隐私权的概念也越来越淡薄，隐私侵权行为日益严重。

第一节 隐私权的发展

隐私是隐私权的保护内容。从历史发展的角度来说，隐私是最先存在的客观事实，然后出现因为人类社会中羞耻心而萌发的尊重私人生活的隐私观念，于是便产生了隐私保护的需求，隐私权应运而生，从法律角度保护个人隐私不受侵犯。作为隐私权保护的内容，“隐私”随着历史的发展和人类社会的进步，逐渐演化出不同的含义，在这一过程中，人类的隐私意识也不断地发展和觉醒。

人类在很久以前就有了隐私观念，并且在此之后的很长一段时间内，隐私都仅仅是人们的观念，并没有演化出多少实质性的内容。在原始社会时，人们就会用兽皮、树皮遮住自己身体的敏感部位，以免在公共场合暴露，后来，人们开始有了道德观念，个人隐私所包含的范围也越来越广，比如有多少钱，在哪里上的学，有没有结婚等。尽管隐私的概念在社会演进过程中有所改变，但其核心的含义仍然是，用户认为是自身敏感的，不愿意公开的信息。

随着人类文明的发展，人们开始有了群居意识，于是出现了村落。由于受地域、交通等条件的限制，大部分村落中的人们很少与外界通信，日出而耕，日落而息，人与人之间的交往并没有现在这么多，大多数人的生活轨迹被限定在一个圈子中，也许是一个村，或是一个镇。这种情况下的人们之间都十分熟悉，每个人的各种隐私信息在“熟人”之间几乎是完全公开的，而在陌生人之间则以一种近乎凝滞的状态缓慢传递，“熟人社会”渐渐形成。因此在这个阶段，并没有多少人在意个人隐私的保护，自然也没有隐私权的说法。

直到 18 世纪工业革命开始，这是隐私发展史上的一个重大突破，人们开始意识到隐私保护的重要性，隐私开始被赋予实质性内容。越来越多的人前往周围的城市工作和生活，城市之间的人口流动开始变得频繁。在这种情况下，人与人之间的陌生程度显著提高，你很可能在自己工作或者生活的环境附近碰见完全不认识的人，人们之间也互相都不了解。这个时期的隐私更多的是私人活动、私人空间和私人信息，例如在自己家里看电影时，别人不应该未经允许的窥视、议论。“熟人社会”开始向“陌生人社会”转化，越来越多的人开始意识到个人隐私的重要性，出现隐私保护的需求，隐私权也呼之欲出。

18 世纪末，随着人们对人格尊严和人格内容的强烈需求，美国学者在论文中将隐私权定义为个人不受外界干扰的权利，这是隐私权作为公民权利的开端。隐私由一种观念形态、事实形态向法律权利转变，隐私权也成为人们作为独立个体享有的基本权利，保护人们的精神利益和部分财产权益。

信息技术的产生，特别是电子计算机和互联网的出现，使得隐私又进行了一次重大发展。各种即时通信手段，比如 QQ、微信，彻底改变了原来人与人之间“口口相传”的信息传递方式，人们认识新朋友也不再仅局限于朋友介绍的方式，通过社交软件中的感兴趣的人推荐，可以轻易认识到跟自己距离遥远的人。互联网与各行各业的合作，使得人们可以不用出门，就可以购买需要的商品、查询想知道的信息、交水电费等。

但与此同时，个人生活的方方面面，比如医疗记录、信用记录、财产状况、犯罪记录也都以数据的形式存在于网络中。网络社会中的个人隐私扩展到了虚拟空间中的电子邮箱、博客空间，甚至一些官方网站上，比如招生网站，与自己有关的个人数据等。而经常与之混用的个人数据是指一切可以直接或者间接识别个人的数据。隐私权保护和个人数据保护的立法目的不同，前者侧重保护个人隐私的权利，后者不仅限于保护数据主体的权利，还要平衡数据主体保护和数据利用之间的关系，促进数据的合理开发和利用。

第二节 大数据时代的隐私特征

与之前描述的传统隐私相比，大数据时代的隐私范围更广，传播速度更快，影响更远，因此在某种程度上可以视作信息时代隐私的升级。一些在传统意义上并不属于隐私的内容，比如姓名、性别、年龄等，在大数据时代也都成了个人隐私的一部分。

由此，我们可以看出，随着大数据等信息技术的发展，个人数据的权利边界日益模糊，个人隐私范围愈加宽泛，个人数据和个人隐私几乎没有差别。因此，本文在大数据的背景下将个人数据全部纳入个人隐私的范围。并将个人隐私定义为："一切与人相关的，可以用于直接或者间接识别该人的信息。包括但不限于姓名、性别、出生日期、户籍、通信地址、身份证号码、护照号码、驾照号码、社会保障号码、电话号码、位置数据、婚姻状况、教育、职业、宗教信仰、网络标识符、金融信息、基因、生物特征和医疗数据。"

大数据时代中的许多隐私都是在日常生活中产生的数据信息，在网站注册填写信息时，在空间上传照片时，在微博发表自己想法时，在购物挑选商品时等，这些隐私内容经互联网记录后成为个人数据，再经过数字化后汇总后形成电子数据库。数据库中的个人数据经大数据分析后，会形成新的或挖掘出其他相关的个人信息，这些信息将被提供给有关部门或企业使用，为人们的生活提供方便。以上描述的流程包括了大数据的生命周期中的发布、储存、分析、使用四个阶段，其中每个步骤都需要严加保护，以防泄露个人隐私。

随着大数据时代人们隐私内容和形式的改变，大数据环境下的隐私特性也发生着改变，使得隐私权的保护难度增大。隐私特征主要有了以下三方面的变化：

1. 隐私范围的扩大化

在大数据时代下，我们的隐私内容范围也变广了，不光传统意义上的住址、财产等敏感信息算是隐私，甚至名字、性别、身份证号等都算是隐私，都不能随意地透漏给陌生人。因为这些本来无关紧要的用户信息在经过大数据的整合分析后，再置于特殊的场景中，就具有了隐私的特性。

也许有人会问，“就算别人知道了我的名字也不一定找得到我啊，毕竟有那么多跟我重名的人。”确实，在多数情况下，仅使用单一的数据如姓名、联系电话，难以对个人进行识别，但是当你的各种单一数据组合在一起，就可以轻易地找到你。根据 QQ、微信等通信软件，可以知道你的朋友圈；网易云、酷狗音乐等音乐平台可以分析出你的音乐喜好；淘宝、京东等购物平台能够根据以往的搜索记录知道你的消费水平和购物喜好；微博等社交软件的“附近好友”功能会暴露你所在的地理位置……当这些数据被组合起来后，大数据可以轻易地找到你。

研究人员曾做过这样一个实验，尝试通过分析一个网站的搜索日志来找出用户的真实身份，搜索日志中包括 1900 万次搜索、1080 多万搜索词以及 65 万余匿名化处理后的用户 ID。虽然这些数据中已经将用户信息删去了，但是通过分析某个用户 ID 所做的一系列搜索，仍然有可能找到这个用户的真实身份。比如他们就根据搜索数据轻易地找到了一位 62 岁的老太太，这个老太太曾经搜索过自己的名字、家乡的名字、60 岁相关的信息。研究人员根据名字猜测是一位女性，之后在数据库中检索某地叫这个名字的人，再加上 60 岁左右、女性的辅助确认信息，很轻易地就确定了老太太的身份（图 2-1）。

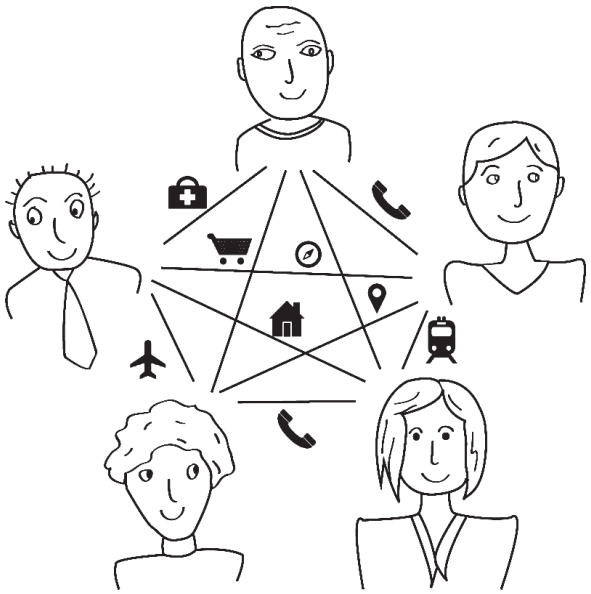

图 2-1　大数据下的信息分析

2. 隐私内容的商品价值化

目前，全球有着数以亿计接入互联网的手机用户，这些用户每天都会产生巨大的隐私数据，如果废弃这些数据，那就是没有用处的数据垃圾，而如果将这些数据收集并用于各种行业之中，这就是大数据技术。在信息时代，对信息的汇集、存储、整理已经覆盖了生活的每一个角落，信息的生产加工与处理已经成为新的创造财富的方法，大量涉及个人隐私的内容被整合入信息之中，成为具有价值的商品。有人说在大数据时代，资本已经不是最有价值的资源了，而信息才是这个时代的黄金。

在过去，隐私泄露的主要危害在于名誉受损，即使存在经济损失也大多是由名誉损失引发的。但在大数据时代，隐私泄露除了造成人们尊严受损，往往也会直接带来经济损失。现今大量用户隐私都被以“个人数据”的形态储存在各类数据库中，包括姓名、性别、身高、指纹、血型、病史、联系电话、财产等一切与个人有关的信息，而计算机和数据库技术

的发展使得人们可以快速、低成本的获取大量信息。于是在这种情况下，大数据时代下的个人隐私信息慢慢变成了一种新兴商品（图 2-2），大量买卖各类信息的渠道出现，买卖的内容包括参加某个展览的人员名单和电话、注册某些网站的用户留下的邮件地址等。各类相关案件层出不穷，“男子贩卖个人信息 8 万条，非法获利 20 万”“19 岁小伙入侵网站，出售上万条用户信息”。

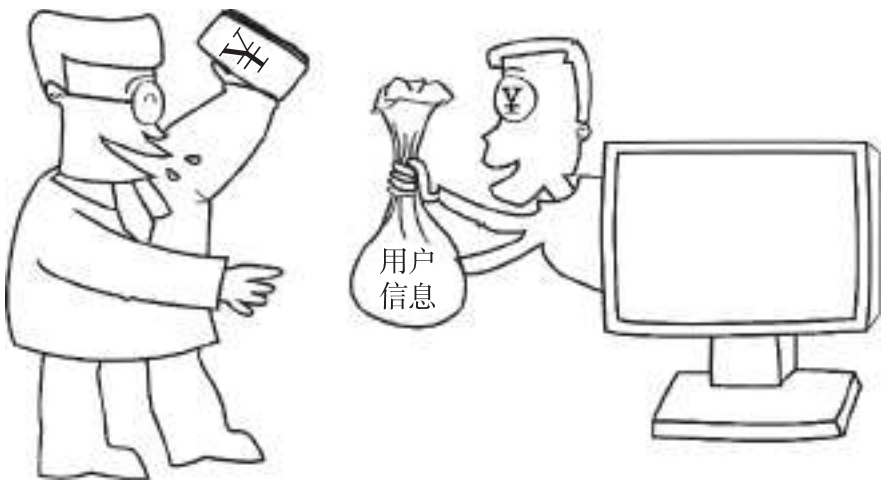

图 2-2　贩卖隐私数据

3. 隐私信息的公用化

为了更好地保护人们安全，国家需要在公路、街道交叉口、闹市区、商场等位置布置大量监控，对摄像头所采集的信息进行大数据分析可以帮助警察识别可疑人物和可疑行为，也可以在犯罪事件发生后以最快的速度追踪到犯罪分子的踪迹，将其捉拿归案。监控的存在无疑为我们创建安全的社会做出了巨大贡献。

然而与此同时，所有人的隐私信息也都暴露在监控面前，甚至现在除了公众场合的摄像头，私人摄像头也被纳入了数据联网，手机监听与网络

监视早已成为大数据信息来源的主要途径。今天你去了什么地方，做了什么事，都可以随时被获取，可能无论你想或不想被别人所知道的事都会被监控记录下来，储存在系统中。在大数据面前，我们的所有举动都将无处遁形。

第三节 大数据时代的隐私权

隐私权是一种基本人格权利，它是指自然人享有的私人生活安宁与私人信息秘密依法受到保护，不被他人非法侵扰、知悉、收集、利用和公开的一种人格权，而且权利主体对他人在何种程度上可以介入自己的私生活，对自己是否向他人公开隐私以及公开的范围和程度等具有决定权。

隐私权告诉我们个人有权对其私人信息进行保密，未经信息拥有者同意不得窥探、搜索及肆意传播，以保护信息所有者的隐私权。大数据时代下的个人隐私权保护的隐私内容主要包含以下三类：

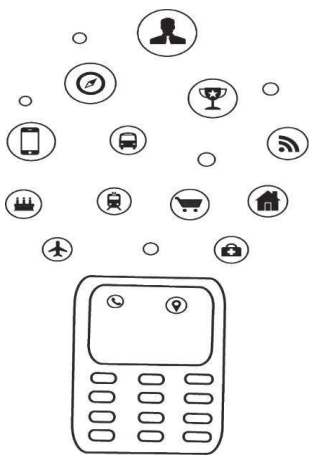

图 2-3 个人信息隐私

1. 信息隐私

这类隐私主要包括人们生活所必备的基本信息，其中包括姓名、身份证号等个人的身份信息、银行账号、家庭及婚姻情况、财产及收入情况、需求和消费信息（如购物、买车、买房、买保险等）、医疗档案、网络上的浏览记录、IP 地址使用情况等活动踪迹（图 2-3）。

2. 通信隐私

这类隐私主要包括人们与他人交流所用的网络平台中发出或收到的信息，其中包括通话记录、发布的微博、微信与 QQ 中的聊天记录、电子邮箱等各类通信方式或网络平台中的信息。

3. 位置隐私

这类隐私是指人们日常工作或生活所处的位置的信息，其中包括工作单位、家庭地址、就读的学校、经常出入的公共场所、出去旅游的地方等描述人们活动轨迹的信息。

由上述内容可以轻易看出，大数据时代人们隐私特征和隐私内容发生的变化，隐私信息范围扩大、来源增多且被赋予商品属性，个人隐私数据被用作大数据交易。这种变化给公民隐私权的保护带来了众多困难，其中核心问题之一是数据所有权的归属，争议焦点是数据源个体所拥有的隐私权与数据控制组织所拥有的数据控制权之间的冲突，比如公民在购物网站上的浏览痕迹是属于公民个人还是属于购物网站。

我国法律对数据所有权的归属并未做明确的规定，主流观点认为个人信息属于数据源个人所有，在原始数据基础上充分匿名化的数据集，企业享有限制性的所有权。

公民的私人信息以及在私人活动和私人领域产生的原始数据应该属于数据制造者，并且可以排除他人使用。这些原始数据是终端用户所存储使用的各种数据，包括网上购物生成的数据、患者病史信息、社保个人账户数据、海关记录的各公司进出口信息、知识产权局记录的申请信息等。组织和企业搜集公民的个人隐私信息时应该被数据所有者授权，并且对这些原始数据进行特殊的匿名化处理，使得数据集中公民的个人人格特征消失，简单来说，就是经过处理的数据看不出这组数据来自谁，切断这组数据与数据产生者的联系。只有获得授权的数据，再经过充分匿名化处理，数据收集、开发者才有可能享有所有权，进行数据交易。

第三章

隐私泄露有什么后果？

第一节 隐私泄露无处不在

随着互联网使用频率的越来越高，我们在网上留下的信息和足迹也越来越多（图 3-1）。无论是在各类网站注册浏览，或是使用购物软件网上淘宝，你的各种信息都在被不知不觉地收集。比如很多人的朋友圈曾一度被支付宝“年度个人账单”刷屏了，殊不知，当你为这些贴心的图片感慨之时，可能已经不经意同意了《芝麻服务协议》的默认选项，允许了支付宝收集自己的某些隐私信息。再比如，有时你需要在搜索引擎上寻找租房信息，进行买票咨询，但没多久就能在预留的手机号码上接到租赁、代购的电话。

图 3-1 用户隐私泄露

也许很多人会说，“那有什么关系，这些信息泄露对我又没有什么影响，我并不在意。”那么接下来我们就从不同的例子介绍隐私泄露到底会对人们产生什么影响，也许在读完之后你会对大数据时代的信息泄露有一个新的认识。

1. 教育信息泄露，人身安全岌岌可危

2016 年，山东女孩徐玉玉被心仪的南京邮电大学录取，然而接下来一通发放奖学金的电话，使她年轻的生命就此定格在了 18 岁。

那天下午，她接到了一通陌生电话，说学校要发放 2600 元的助学金给她，这对于她本不宽裕的家庭是一笔意外收入，在又接到“教育部门”的电话，让她办理了助学金的相关手续后，她开始对这件事确信无疑，并将学费 9900 元打入了对方提供的账号中。然而直到等了几天也没有等来说好的助学金，打入的学费也不见了踪影，她才意识到自己可能是被骗了。案发后，徐玉玉与父亲到公安机关报案，但在回家的途中心脏骤停，送到医院抢救两天两夜后死亡。

通过警方的侦查，我们了解到在这起案件中，犯罪分子通过网络购买了学生信息和公民购房信息，并分别在山东、海南、江西等地，冒充教育局、财政局、房产局工作人员，以发放贫困学生助学金、购房补贴为名，以高考学生为主要诈骗对象，拨打电话，骗取他人钱款（图 3-2），涉案金额共计人民币 56 万余元，通话次数共计 2.3 万余次，影响范围巨大，性质恶劣。

图 3-2　教育信息诈骗

虽然事到如今，所有犯罪分子都得到了严惩，但是徐玉玉的父亲仍然难以走出丧女之痛的阴影，妻子也一

病不起，大女儿从新加坡辞职归来，至今全职陪护。他说，在这些犯罪分子中，自己最痛恨倒卖玉玉信息的人，因为没有他们，就不会发生后面的事。

自徐玉玉被电信诈骗案件发生后，人们开始关注原来并不在意的个人隐私信息严重泄露问题。也许有人会好奇，一个准大学生为什么会轻易地相信电话中的诈骗分子？其中最主要的还是因为骗子准确地说出了她的身份证号码、家庭情况、银行账户、助学金申请信息等被认为是特定机构的特定人员才能了解到的情况，而对隐私信息的核对本身就是普通人常用的一种确认身份的方式。徐玉玉用生命为代价，诉说出隐私安全的重要性，为我们敲响了警钟。

2. 超市购物记录泄露隐私，信息安全荡然无存

相信我们都或多或少的收到过超市的优惠广告，在大数据技术还没出现的时候，超市只是将一样的传单随机发放，而现在，超市可以通过大数据分析每个顾客的需求，精准推荐商品。

一个典型的例子发生在美国的超市塔吉特百货公司。由于美国的婴儿出生记录是公开的，因此在孩子出生后，新生儿母亲就会被铺天盖地的产品优惠广告包围，如何在众多优惠广告中突出重围，并吸引到孕妇这一消费能力很高的群体，成为各家超市思考竞争的核心问题。

虽然商场有各类用户购物数据，但是怀孕毕竟是私密信息，如何准确判断哪位顾客已经怀孕成为了很大的难题。塔吉特顾客数据分析部的高级经理安德鲁斯在对已有的塔吉特的迎婴聚会登记表中的顾客消费数据进行建模分析后发现：许多孕妇在第 2 个妊娠期购买大量的无香味护手霜，在怀孕最初的 20 周会购买大量补充钙、镁、锌的善存片类保健品，最后安德鲁斯选出了 25 种典型商品的消费数据构建出一种“怀孕预测指数”，这个指数可以在很小的误差范围内预测顾客的怀孕情况，以便于超市早早把孕妇优惠广告寄给顾客，占据先机。公司的营业额从此借助数据挖掘稳

步上升。

然而这个举动虽然使商家获利不少，但这在一定程度上也暴露了用户的隐私。2012 年，美国一男子闯入他家附近的零售连锁超市塔吉特内抗议，“你们竟然给我 17 岁的女儿发婴儿尿片和童车优惠券”。之后他却发现，自己上高中的女儿确实怀孕了，超市比他这个父亲还提早一个月发现。

大数据时代下，凡是我们走过的地方，身后都会留下一片数据，人们不由开始担心自身的隐私泄露问题（图 3-3）。我们无法不让大数据知道我们发生了什么，即使是怀孕这种隐私的问题也可以被分析出来。超市在隐蔽的情况下记录消费者的购买喜好，其本意是好的，为了提高超市销售量，同时也提升人们的购物体验，但我们不知道还能从这些数据中分析出别的什么隐私信息。如果商家收集的用户数据没有被妥善保护好，被不法分子获取利用，从事电信诈骗、非法讨债甚至绑架勒索等犯罪活动。甚至有些企业还将消费者个人信息视作公司财产，打包出售给大数据公司或广告商，作为商家牟利的工具，这将会对消费者的人身安全、财产甚至名誉造成巨大威胁。

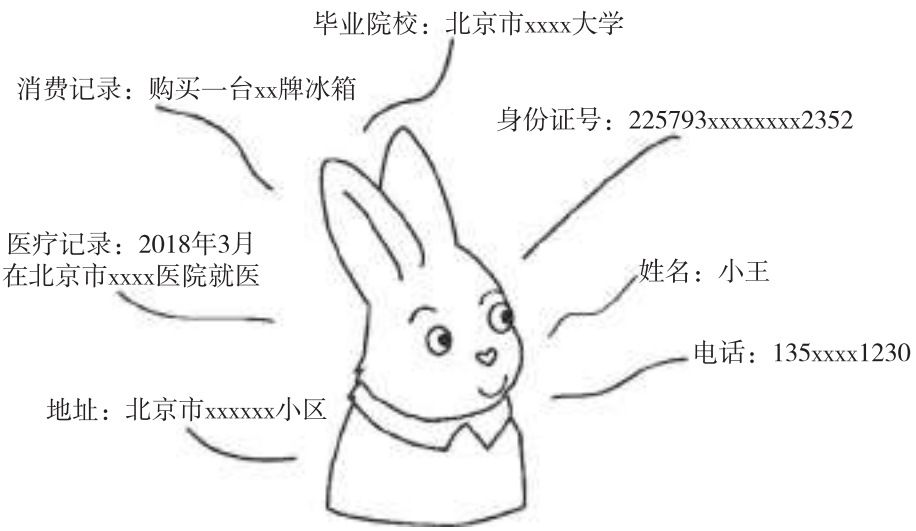

图 3-3　网络上的个人信息

3. 电信诈骗升级换代，财产安全如履薄冰

无论从前还是现在，婚姻都是一个人甚至一个家庭的大事。旧时人们遵循“父母之约，媒妁之言”，现在随着时代发展，人们观念开始改变，大家开始推崇自由恋爱，但现代社会的生活节奏很快，大多数年轻人都忙于工作，没有时间去认识新的适合自己的人群。于是在这种情况下，相亲网站出现了。

为了更好地为用户介绍可能感兴趣的人，大多数的相亲网站需要注册人填写姓名、学历、财务状况等隐私信息（图 3-4），大数据技术在采集所有用户信息后，会自动为用户推荐符合要求的适合的相亲对象，使用大数据技术后，人们对相亲对象的满意度大幅上升，成功率也越来越高。然而，在相亲网站大肆盛行的情况下，也有一些不法分子看到了其中可以利用的漏洞。

最近这些天，王女士的烦恼不断，她怎么也想不明白，自己支付宝里的 3 万元到底是怎么丢的。故事还要从几个星期前说起，由于工作繁忙并

图 3-4　相亲网站诈骗

且已经到了适婚年龄还没有合适的对象，在父母的催促下，前些天她就在某相亲网站注册了用户，并发布了信息，相亲网站的效率倒是很高，没过几天，她的手机上就收到了一条提醒短信，写着“王女士，您好，我在某相亲网站上看到你的信息，感觉您非常适合我，希望和您交朋友，这里面有我的照片，请你点击看一下。”看到这里，王女士没多想就点了进去，但是并没有图片，只是一个不相干的下载网页。她最开始还以为是有些人的恶作剧，直到收到一条消费短信，提示她说银行卡里的 3 万块钱已通过支付宝支付，这令王女士十分惊讶，她最近并没有类似的大额的消费，于是赶紧向银行查询自己的余额，结果被告知，3 万块确实已经被划出，这时她才意识到，可能是几天前的那条短信出的问题，连忙报警。

经过警方的调查，犯罪分子通过网络获取了大量的此相亲网站上的用户信息，并群发了上述相似的短信，受害者在点进链接的时候，就会下载犯罪分子构造好的木马。趁受害人熟睡之时，犯罪分子通过植入的木马将王女士的手机关机，再利用王女士的账户转账。当付款需要输入密码时，犯罪分子会点击忘记密码，然后通过银行预留的手机号申请短信验证码。而含有验证码的短信就会被木马截取，发送到犯罪分子那里。经过一系列的操作，王女士银行卡里的 3 万块钱就被神不知鬼不觉地转到犯罪分子手中了。

第二节　隐私保护新挑战

在当今这个时代，大数据记录着我们生活的点滴，我们的个人隐私在大数据面前变得无处遁形。一个人从出生、上幼儿园、上学、就业、结

婚，到网购、开公司、体检、买车，每个环节的各种数据都在被采集。无论是说过什么话，做过什么事，有什么爱好，还是生过什么病，有什么亲朋好友，可以说，只要我们自己知道的它几乎都知道，甚至我们都没有意识到的事，它也可能知道，比如在跨门槛时喜欢先迈左脚，在聊天的时候喜欢加微笑表情，集体照相的时候更喜欢站在旁边，等等。因此大数据技术又被称为“网络时代的科学读心术”，它通过把人的特征、行为、选择等信息化为人类生活提供某些便利。

互联网虽然为我们的生活提供了许多便利，但也让我们在这个时代里不得不“裸奔”。随着恶意程序、钓鱼等各类黑客技术的发展和不法分子的利用，大量网民的基本个人信息、设备信息、账户信息、社会关系信息和网络行为信息等都由此泄露，与之有关的各类财产损失案件不计其数。比如近年影响范围很广的携程和 12306 用户隐私泄露事件，造成了大量用户的密码、手机号、邮箱等信息在网上传播，更严重的是一些用户为了更方便地记忆密码，习惯在各大网站都使用同样的密码，一旦密码泄露，则在所有网站的信息都将暴露在不法分子的面前了。大数据技术的发展给隐私保护带来了前所未有的挑战，主要包括以下方面：

1. 隐私边界模糊

隐私是一个主观概念，它根据不同的人、不同的时间变化而变化，因此难以对其定义和度量。在大数据时代，数据分析追求全数据、混杂性、相关关系和数据化，这大大地拓宽了个人信息的范围，除了传统的姓名、性别信息数据外，个人的互联网大数据、传感数据、行为数据、地理位置数据等，都在被纳入信息收集范围，个人信息和隐私的边界被进一步模糊，个人信息和个人隐私面临着被无限制、无差别收集和使用的风险，信息主体享有的知情同意权、异议权、更正权、删除权等，往往得不到充分尊重和保障。

2. 信息越界搜集

大数据时代，人们使用智能设备进行社交、获取信息以及休闲娱乐，生活中早已离不开它。但是智能设备在使用时需要装上各种功能的应用软件，我们在安装这些软件的过程中往往会面临这样的困境，无论软件提供的服务是否需要，几乎所有的权限都要求被提供，包括位置信息、读取短信、调用通信录、开启摄像头等，并且软件开发者并未告知用户这些权限的用途。比如，在安装一款录音软件时，为了提供更好的服务，软件要求读取麦克风设备无可厚非，但是如果需要读取位置信息、通话信息或者是短信信息就是越界收集信息了。可怕的是，据调查这类点击同意被默认侵犯隐私的用户占到了安卓手机用户的 47% 以上。而苹果的 iPhone 手机长期记录用户地点位置的特性也曾引发过关于侵犯隐私权的争议。

3. 隐私侵权问题严重

传统的隐私侵权行为主要表现为窥视、监听、监视、刺探、口头宣扬、书面传播等方式，这些行为大多需要的技术程度不高，专业性不强。而大数据时代的隐私侵权行为在很大程度上依赖于先进的设备、软件和技术，以技术性较强的方式进行。网络的应用与普及大大增强了人们获取、处理信息的能力，各种收集、分析人们隐私的行为使得获取人们信息的渠道增多，比如现有的网站普遍都使用 Cookies 将用户提供的信息都记录并存储下来，甚至有的企业还利用 Cookies 偷偷记录用户的浏览记录，用户的隐私信息因此存在着被不当利用和泄露的危险。另外高端信息技术的发展，如 GPRS 全球卫星定位系统、可视通信技术等也给隐私侵权提供了更大的可能性，我们的位置可以实时被记录，各种信息都暴露在高科技面前，隐私侵权问题相当严重。

4. 信息量剧增

大数据时代，人们无时无刻不在产生数据，通信数据、网站数据、位置数据等，个人信息数据的规模高速增长、数据特征错综复杂。并且这些信息具有不同的维度，如通信信息暴露你的社交状况，购买能力暴露你的财务状况，购活动轨迹暴露你的生活习惯等，这些个人信息还与政府、企业、网站平台以及其他的个人信息相互关联，通过数据挖掘和分析，这些飞速增长的数据信息具有极高的价值。随着个人信息数据剧增，个人信息的收集方式、传播渠道及使用后果日趋失控，个人信息安全问题比较严峻，有效保护难度较大。

5. 影响扩大化

互联网的广泛应用打破了地域与时间的限制，信息的传播范围更广、流通量巨大、流通速度惊人，数据背后蕴含着巨大价值。因此一旦隐私侵权的行为发生，有可能给受害者的名誉造成难以挽回的影响和伤害。大数据的飞速发展使许多不法分子看上了这块保护还不够严密的“馅饼”，近年来隐私泄露事件频繁发生，涉及的人群基数也较大，每一起事件都在社会上造成了很大的影响，比如铁路购票网站 12306 漏洞危机、连锁酒店多达 2000 万条客户开房信息遭泄露等，已经有越来越多的人意识到隐私保护的重要性。

第三节　隐私泄露影响广泛

网络支付和电子商务的发展迅速使得每个人的信息具有了更大的商业价值，在这种情况下发生的隐私侵权行为有可能导致更加严重的经济损失，比如用户可能会因为在不安全的网站购物而面临银行卡账号和密码被盗的危险等。简单来说，隐私泄露对我们生活的影响有以下几种：

1. 侵犯隐私权

在越来越拥挤的社会生活和星罗棋布的监控生活中，信息收集和数据监控混淆并淡化了私人领域和公共领域之分，本应是权利主体的公民却变成了不断被处理的数据客体。隐私信息一旦泄露，首先侵犯的就是信息主体的隐私权，这种行为不仅是对信息主体尊严的践踏，而且还将造成社会性的恐慌。

2. 垃圾短信、骚扰电话和垃圾邮件

这已经是这几年来十分普遍的一种情况，本来只是私人使用的电话号码，只是在一些网站、银行留过后，就开始接受无尽的垃圾短信和推销电话，用于用户注册的邮箱也不能幸免，各种垃圾邮件多到影响邮箱正常使用（图 3-5）。

图 3-5　垃圾信息骚扰

3. 冒名办卡、冒用身份、名誉受损

当你的身份证等个人信息被人掌握后，不法分子就可以通过办理你的身份证，申请各大银行的信用卡并透支消费，或者挂失你的银行卡，重新设置密码使用，甚至还可能利用你的个人信息进行违法犯罪，损害你的金钱和名誉（图 3-6）。

4. 诈骗

随着互联网的发展，传统的电信诈骗也开始升级，不法分子在掌握你的隐私信息后，通过冒充学校、公安、政府部门等，进行更有针对性的诈骗，使人防不胜防（图 3-7），造成极大的经济损失。

5. 各类账户密码被盗

随着科技的发展，不法分子可以破解的密码难度越来越大，破解同等难度的密码所用时间越来越短，账户安全形势严峻。也许有人会说：“这和我有什么关系，密码被攻破之后我还可以再换一个密码啊，又不会对我造成多大的影响”。下面我们通过对几种常见账户被攻破后可能带来的安全隐患分析，让大家对账户安全风险有更深的了解。

（1）社交网络账号被攻破

如果你的社交网站用户账号被攻破，那么就可能被不法分子用来发布一些意想不到的敏感信息，比如发送垃圾广告、传播病毒，甚至冒充你与你的朋友通过聊天行骗。给你的朋友、同事和你自己带来重大的伤害。

除此之外，还有可能获取个人敏感信息，比如电话、邮箱以及身份证等注册信息，这可能成为你不断接到骚扰电话、垃圾邮件以及诈骗电话的原因，给个人生活带来极大困扰。

（2）电子邮件用户账号被攻破

如果你的电子邮件账号被攻破，首先面临的后果就是重要的邮件被窥

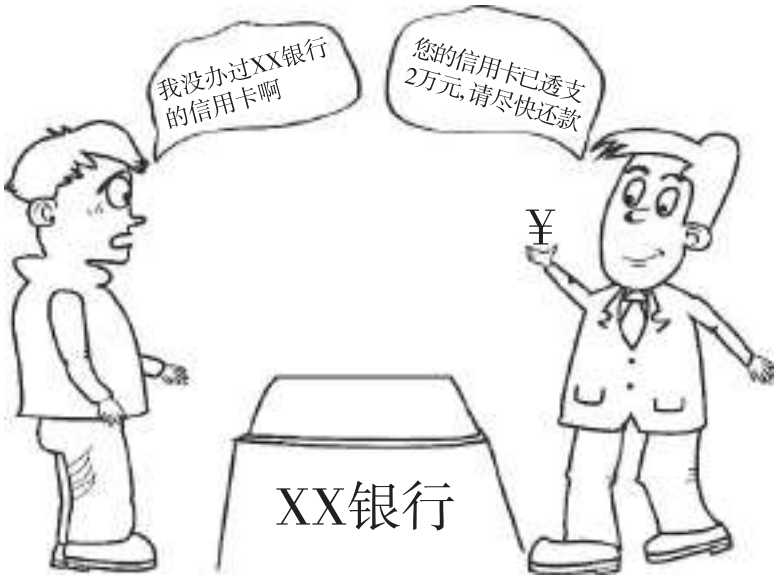

图 3-6　身份冒用

图 3-7　电信诈骗

视。电子邮件已经成为许多个人、企业及机构传递信息的重要工具之一，其中不乏重要的信息，如合同、身份证、银行账号及网站账号申请的确认信息等。邮箱账号被攻破后，其中的合同、身份证等信息可能被用于诈骗，特别是电子邮件中的银行账号及网站账号申请的确认信息更是有可能成为潜在危险，引发其他账号被盗的严重后果。除此之外，不法分子在攻破你的电子邮件账号后，可能用于发布垃圾广告、传播病毒及敏感信息。

（3）网上银行用户账号被攻破

如果不法分子攻破你的网上银行账号，加之你网上银行账户设置的安全措施不到位，他们将会肆意消费网上银行里的钱或者将钱转到其他账号上，甚至可能通过这些账户信息办理信用卡或者贷款服务，通常会给持有人带来较大的经济损失和名誉损失。

（4）办公系统用户账号被攻破

如果你的办公账号被盗，不法分子很可能将其中的重要文件内容修改，并且发布诽谤、中伤他人的内容，还可能发布虚假的任职公示、加薪通知，给单位和同事造成混乱和困扰。更严重的情况是，单位的一些重要文件可能会被不法分子窥视，甚至窃取、倒卖。

（5）系统管理员账号被攻破

如果你是系统管理员，你的账号通常拥有相当高的权限，一旦你的账号被攻破，这意味着不法分子可以随意利用系统管理账号进入相应的系统，通过高权限修改其他账号的权限，增加或删除有关账号，窃取文件更是易如反掌。

第四章

隐私是怎么泄露的呢？

生活中你是否有这样的经历：想买车了，朋友圈就能收到汽车 4S 店的广告；刚有买房的意向，就接到了房产中介的电话；上午还在看新出的手机型号，下午电子邮箱就被手机供应商的广告塞满……你是否也会疑惑，商家何时拥有了这样的“魔力”，可以随时洞察我的消费意向？他们又是从哪里获知了我的个人信息？下面将从个人泄露、数据窃取、手机入侵、恶意程序和网站漏洞五个方面解答这些疑问，分析大数据时代隐私泄露的途径。

第一节 个人泄露

1. 社交网络

与传统隐私泄露的方式不同，大数据时代下的隐私泄露大多发生在日常生活中人们没有意识到的行为：浏览记录、分享的照片、网购的商品、看过的视频网站、无意间填写的各种信息都会成为隐私泄露的来源。这些信息一旦产生，就会被长久储存在网络空间中，即便你已经在自己的设备上删除掉了，这些记录也将继续成为大数据分析的素材。

移动互联网的发展带动了社交网络的盛行，现今很多人都喜欢在微信、微博中分享自己的生活，比如去哪里旅游了、与好久没见的朋友逛街吃饭等。然而这些看似无关紧要的照片中实际存在着很大的安全隐患，发布的每一条心情的定位都暴露着你的位置信息，你与好友的相聚照片透漏出你的交际圈，如果这些信息被有心之人利用并泄露出去，可能你的生活从此受到影响，甚至蒙受财产损失。因此，社交网络成了个人敏感信息泄露的“重灾区”。

下面通过一个简单的例子，帮助你更加深刻地理解大数据时代下社交网络中的你所不知道的潜在威胁。

今年 30 多岁的李先生是一个社交达人，喜欢在社交网络上分享自己的生活动态，比如在孩子学校的亲子活动很开心，这家常去餐厅的味道不错，但李先生并未想到这次的动态分享会造成家中的经济损失。

随着孩子暑假的来临，自己也终于得到休假，李先生决定带家人一起去国外旅游放松一下，他习惯性地在社交圈中分享了自己的行程，并晒出

多张旅途中的全家福照片。结束行程的他回到家后大惊失色，发现家中价值 10 万余元的财物被盗（图 4-1）。

图 4-1　旅途信息泄露导致财物被盗

案件被警方侦破后，被抓捕的盗窃者交代，他是在社交网络上看到了李先生分享的全家福照片，随后对照片中包含的位置信息进行了技术分析，确认李先生的位置在国外，并且家中没有其他人后入室盗窃。

从“原图”中恢复出李先生的位置信息，这听起来很不可思议。那么“原图”为什么会暴露个人位置信息等隐私呢?

事实上，现在的智能手机拍摄的照片，都含有一个叫 Exif 参数的东西。参数中包括光圈、日期时间等各种图像数据，还包括最关键的暴露我们个人位置的位置信息。我们在日常拍照时，都需要调用 Exif 中的 GPS

全球定位系统数据，这些来自手机内部的传感器数据，照片在储存时也会自动把拍照时的位置、时间等信息一点不差地记录了下来。

于是当你将“原图”发在社交网络时，这些附加信息也就一并被发了出来。那种“我发照片时关键信息都打了马赛克，所以很安全”的想法已经过时了，这种简单的处理方式对不法分子来说都不是问题，仅通过一些普通图片处理工具，别人就可以很轻松地拿掉马赛克，恢复原始的图片信息。

此外，“附近的人”功能也是人们不小心泄露隐私信息的重灾区。这个功能本身是为了给喜欢交朋友的人提供一个平台，帮助位置接近的人们相互认识，因此会定位你的位置信息。安全专业人员曾经做过一个实验，通过“查找附近的人”的功能，多次定位自己与目标对象的距离，并通过简单的技术处理，就可以确定目标的准确位置。有些手机的系统中还含有“常去地点”的功能，可以通过地图显示你常去的位置。

现实生活中，很多人贩子在行凶作案时，与被害人素不相识，但是能将孩子和妈妈的名字叫出来，还有两人的照片。原因就在于，家长经常在社交网络上发表与孩子互动的日常照，这些日常照片中包含着自己的家庭关系，并且家长没有关掉微信中“附近的人”这个设置，骗子使用微信“附近的人”这个功能，来成功获取被害者信息。

然而有的人会疑惑，朋友圈中泄露的只是部分的信息，而且还是零散的、不确定的，这些信息怎么就能确切地与自己对应起来，并且分析出自己的其他隐私信息呢？并且，随着各类安全事件的发生，人们对于大数据时代下隐私信息的安全性愈加关注，不会轻易把个人的关键信息放在网上，隐私为什么还会如此轻易地被泄露呢？

事实上，你放在社交网络上的个人信息远比你想象的重要和广泛，取完快递后随手丢下的快递单中包含你的姓名、电话、住址和购物习惯等信息，开心地晒在社交网络上的火车票、登机牌中包含你的身份证号、姓名，将这些零散的用户信息进行大数据的整合分析后，很容易就可以找到

你并继续挖掘你的其他隐私数据。而个人隐私的泄露除了自己无意之间放到网上的个人信息被他人不当获取之外，通过大数据对你在网络上记录的汇总、分析，也可以对一些比较隐私的个人关键信息进行有效推断，比如年龄和性别等信息。

人们在社交网络上的一举一动，比如你浏览网页的记录、聊天表情的使用频率，都是性格特点与内心状态等心理特征的某种反映。个人往往不需要在社交网络上直接写下“我是什么性格的人”，只要对社交网络的日常使用积累到一定数量，科学家就能够运用大数据分析技术，通过其在社交网络上日常展示的信息自动计算出心理特征，甚至还有可能识别出个体的性取向、政治倾向、价值观等通常意义上更“敏感”的个人信息，如果我们在社交网络上展示的内容足够丰富，对我们心理特征的计算可以做到很准确，甚至能超过家人对我们的了解程度。因此，只隐去传统意义上的个人关键信息，在大数据的分析下，可能我们的隐私反而会以一种更深刻的形式泄露出去。

2. 人肉搜索

“人肉搜索”指的是出于某种目的，比如说被网络骗子给忽悠了，想找到对方的联系方式，于是一大帮“热心”的网友自发组织起来，利用各种途径利用网络检索的方法找到他在现实生活中的各种数据。尤其是在大数据时代，信息的海量性和流通性扩大，获取一个人的信息变得更加简单。在找到零散信息的基础上进行聚合加工，将信息的生产、传输、聚合等端点联系起来，很快就能找到你的信息。有人会说，这太不可思议了，就凭这么一点信息，就能在那么多人找到我？看完下面这个故事，你应该会知道，生活在大数据时代，为什么你的隐私信息那么容易就被获取。

一天，满面春风的领导叫住小张，说是要给她介绍相亲对象，兴奋的小张开始幻想“哪里人？多少岁了？有照片吗？”但无奈，领导只留下

“小王，××公司的，我只知道这些”，轻飘飘地走开了。于是，小张陷入了深深的沉思，应该怎么样才能提前知道他的个人信息呢？

小张首先打开搜索引擎，输入“小王+××公司”作为关键词，惊喜地找到了小王的人人网动态，于是先从人人网下手，点开主页一看，发现了此人爱好游戏、篮球和天文，并且在一大堆帖子中，找到了一张图片，图片右下角的水印显示出了他的微博地址，激动之余，小张立即在微博中搜索他的动态，在微博动态中不出意外地发现了他日常生活的照片和动态，比如“大数据技术与人工智能的结合真是厉害”“两天辗转三个城市，好累”“好久没有周末的我，窝在家里打游戏真是太幸福了”。另外，小张竟然还在一家招聘网站找到了一份小王的求职简历，毫无意外地在上面发现了小王的年龄、联系方式、住址甚至是家庭关系。此外，她还在易趣、淘宝、天涯社区、新浪论坛等，找到了小王的一些其他信息。

这样一来，小王的形象瞬间变得立体起来，个人信息和兴趣爱好几乎全部可以预见。除个人信息外，小张对小王的形象便停留在业余爱好是游戏，另外根据微博频繁晒出的行业信息、行程分享可以看出，这无疑是一个标准的技术男，且经常出差，是一个辗转各地的“空中飞人”，这与小张的择偶标准相差甚远，见面这件事情也就不了了之。

事实上，这是一个精简版的“人肉搜索过程”，个人利用各种资源渠道，尽可能多地搜集目标任务的所有信息，但是这些信息并没有被公布，基本不会对当事人的生活造成失去一次相亲机会以外的影响，但真正的人肉搜索往往会给当事人带来极大的精神伤害，甚至是人身危险。

以“剥光”为终极目的的人肉搜索引擎，就是群情激愤下的一把双刃剑。当这把双刃剑被成千上万的网民以道德之名举起时，它既可以揭露真相，比如最牛房产局长“周久耕”，网络炫富女“郭美美”。但同时，也可能变为不明真相下的肆意伤害，比如扶摔倒老人的“彭宇”，眼癌女童“王凤雅”。但无一例外，人肉搜索的最终结果就是被搜索对象的所有个人隐私全部被曝光在网络上，就像被人扒光衣服浑身赤裸地待在公共场合，

受到各种方式的议论，个人安宁遭到破坏，精神受到伤害，甚至生命受到威胁。

他们将被搜索对象所有的信息经过整理，反馈到网络上与其他人分享，接着，大家在已有信息的基础上，再接再厉，交叉、重复地进行信息的收集、加工、整理等工作，并将信息再次分享给遍布在网络那头千千万万的战友，这时候可以说，那些你曾经留在网络上不以为意的信息碎片，被轻易地获得、聚合、更改、利用，可以轻易得到你的姓名、年龄、兴趣爱好、居住地点、家庭状况甚至祖上三代的信息。

随着大数据技术的日益发展，计算机取代了网友搜集信息的工作，数据的搜集不再依靠无数网友在线上、线下的调查、分享，而是计算机伸出无数的触角在互联网上寻找你有意无意在网络上留下的痕迹，比如你订票、订酒店的信息，网络购物的信息，微博上的日常动态，论坛中的各种观点等，之后将这些痕迹数字化后保存在数据库中，这些数据变成为分析你个人基本信息、心理特征的数据来源。而网友用的那些数据搜集和整理的方法被无数越来越精准的算法代替。因此，分析的数据来源变得更广，速度更快，对于信息挖掘的精准程度也越来越高。

第二节　数据窃取

1. 非法倒卖

大数据时代下，数据对于企业来说都存在着巨大的价值，而作为数据资源的核心组成部分，数据已经成为了很多企业愿意买单的“产品”。企业使用大数据技术将客户打上不同的数据标签，形成个人和企业用户画

像，再根据不同业务需求，甄别出目标客户群体，比如针对用户消费喜好的个性化营销，挖掘具有潜在消费的客户，利用大数据技术和应用帮助企业开源节流，在解决自身业务需求和问题的基础上大大降低企业的总体投入成本。

有了需求，自然就会有市场，在各路企业对各类数据虎视眈眈的前提下，数据交易市场得到迅速而野蛮的发展，交易数据的种类包括政府、医疗、金融、电商、能源、交易、交通、商品、消费、信用卡、教育、社交、社会等各方面，各类数据的非法交易越来越猖獗，给社会和群众造成了难以估量的损失。

一个手机号码 2 元，一张征信报告 300 元……财产信息、户籍信息、计生信息等各式各样的个人信息被明码标价，买卖双方不问来源、不问用途，在信息贩卖者眼中更没有“隐私”二字，只要有利可图，隐私数据就被随意买卖。

32 岁的龙某是湖南人，之前从事信用卡催收工作，因工作需要，常常在网上购买欠费卡主的个人信息用以催收。接触到个人信息买卖后，龙某被其中的暴利吸引，动起了歪心思。之后，龙某辞职与女朋友何某一同前往拉萨，利用原来的工作关系，收集大量的计生信息、户籍信息，稍加整理后将信息贩卖，仅两个月，两人就非法获利近三万元。

这样贩卖隐私信息的案例绝非个例，杜某原在某工程集团担任驾驶员，因嫌工资低，在贩卖信息的道路上看到了“商机”。于是他经常从上家龙某手上打包收购各类信息，卖给某商贸公司老板。该商贸公司名义上是做贸易的，事实上却是贩卖个人信息的，其贩卖的信息包含姓名、单位、住址、联系电话、名下房产、车辆信息、银行贷款及不良信用记录等多种信息的征信报告。

那么，卖家的个人信息库从何而来呢？总的来说，这些贩卖的信息来源主要有三种：

（1）黑客攻击

图 4-2　黑客盗取隐私信息

个人信息被倒卖事件屡见不鲜，很重要的原因就是随着互联网技术的发展，网络黑客入侵重点网站窃取信息的可能性增大，对政府机构、大型国企、高校、电商、交通等重点客户进行攻击的手段日益多样化，而掌握大量公民个人信息的一些机构网络安全防护意识不强，投入不足，特别是没有对不断出现的网络安全漏洞及时采取修复措施，很容易被黑客攻陷，造成大规模信息泄露（图 4-2）。

在生活中，我们常听到的“暴力破解”和“密码撞库”也是黑客获取用户账户信息的重要方法，那么“暴力破解”和“密码撞库”究竟是什么，一起来了解一下吧！

首先是“暴力破解”，也称作“密码穷举”，这是黑客攻击用户密码最基本的破解技术。如果黑客事先知道了账户号码，如邮件账号、QQ 用户账号、网上银行账号等，而用户的密码又设置的十分简单，比如用简单的 4 位数字组合，则最多有 0000 到 9999 一共 10000 组密码，黑客使用暴力破解工具很快就可以破解出密码来。除此之外，弱口令密码字典破解也是暴力破解的常用方法，黑客使用弱口令密码来缩小密码范围，加快密码的破解速度。弱口令密码字典是黑客将常见的数字和字母的组合收集起来组成的密码集合，比如英文单词以及生日的数字组合等，表 4-1 列举了一些常见的弱口令密码。

表 4-1 常见的弱口令密码

000000	111111	11111111	112233	123123	123321
123456	12345678	654321	666666	888888	abcdef
abcabc	abc123	a1b2c3	aaa111	123qwe	qwerty
qweasd	admin	password	p@ssword	passwd	iloveyou
5201314	asdfghjkl	66666666	88888888		

其次，“密码撞库”是近年兴起的一种针对数据库的攻击方式，黑客通过搜集互联网上已经被泄露的用户名和密码信息，尝试批量登录其他网站，得到一部分用户在其他网站的登录信息。简单来说，就是黑客可以在攻不破 B 网站，但又想得到 B 网站的用户信息时，尝试攻破与 B 网站有关联的、安全性较差的 A 网站，然后用 A 网站的账户信息尝试登录 B 网站，因为很多用户在不同网站使用相同的账户密码，所以极其容易成功。大家所熟知的苹果公司 iCloud 账号被攻破，一大批明星照片被曝网络的事件就极可能是黑客使用“密码撞库”的结果。

网络安全专家介绍，当用户很少在不同的网站使用相同的密码时，“密码撞库”成功的概率就会很低，反之，成功的概率就会大大提高。但不幸的是，很多用户都是后者，在各种网站使用了相同的账户名和密码，比如在网购、QQ 或者是论坛等各种社交工具和电商网站中使用相同的账户和密码。虽然网购网站和论坛网站属于两个互联网公司，用户的数据也储存在不同的数据库中，但是黑客盗取一个网站中的用户数据后，就可能匹配出使用相同密码的其他网站的用户数据。这种犯罪的成本和手段都相当简单，不法分子能够屡次得逞的主要原因还是用户为了方便或者是好记，在不同网站使用相同的登录密码。

（2）内鬼贩卖

为了得到更好的服务，很多时候用户会向特殊的服务机构提供自己的

个人信息，比如向教育机构提供姓名、年龄和知识水平信息，向汽车 4S 店提供汽车牌号和驾照信息，向金融机构提供身份证件和财务情况信息，因此，这些服务机构内部数据库中有大量用户的隐私信息，一旦这些机构对用户的信息数据监管不力，员工将数据擅自披露或售卖他人，就会造成用户隐私数据泄露。

（3）信息整合

一堆毫无交集的数据，经过大数据技术的处理、交融，可以得到大量的隐私信息，使得包含隐私数据信息的价值得到提升，这也成为挖掘隐私的新办法。因此，用户有意无意留下的各种痕迹会被搜集，比如废弃的火车票中的姓名、身份证号，包裹上快递单上的地址、联系方式，这些信息被搜集、处理、分类后成为具备价值的商品，流通在市场上并被用于各行各业（图 4-3）。

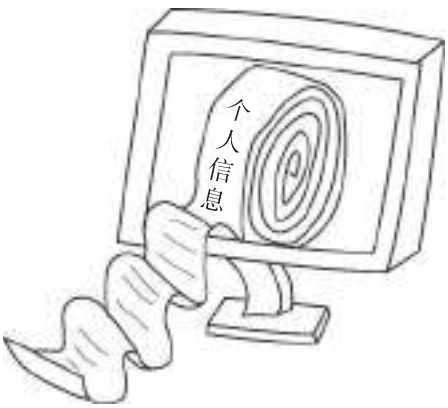

图 4-3　大数据下的信息整合

2. 第三方泄露

隐私泄露风险的增加，很大程度源于个人信息被暴露的环境和应用场景增加。比如当你看到网站上邀请朋友点赞赢礼品活动时，满怀期待地将邀请到好友的个人姓名、电话、地址等信息发送给客服人员，但却迟迟没有收到所谓的礼品，反而在一段时间后收到大量的垃圾短信和营销电话，我们的隐私信息就这样被第三方借助某些手段搜集了。

在移动互联网时代，用户难免要牺牲个人信息以获取一定的服务，有些甚至是不自觉行为，比如你只要浏览了电子购物网站，你的购物信息就会被获知。此外，在大多数应用场景都要求实名制的今天，各大平台掌握了用户大部分的信息，比如手机号、身份证号等。同时，基于基站和

GPS 技术，平台能够轻易而准确地知道你的地理位置信息，手机联网之后的设备信息自然也无处可逃。互联网在提供生活便利的同时，也让用户成为了不折不扣的“透明人”。

当你在社交网络中看到“想知道你是一个什么样的人吗？点进来看看吧！”时，你怀着好奇和怀疑的心态同意授权测试，测试结果给出一个和你想象中的自己异常契合的结果，于是你开心地将测试结果分享到社交网站上，并顺手 @ 了几位好友。你在做完这些事情后并没有发现任何不妥，但是在你同意授权测试的时候，第三方平台就获取了你注册社交网络时的个人信息和你在社交网络上的行为轨迹。

事实上，确实曾有一家公司在社交网站上发布了一个专门用作性格测试的第三方小程序，用户不仅可以免费参加测试，而且匿名捐献自己在社交网络上行为数据作为研究使用的参与者还可以获得一定的酬劳。这个小程序取得了巨大的成功，有 600 万用户使用过这款小程序，其中一部分用户同意捐出他们在社交网络上的行为数据供研究使用。之后，数据搜集者不仅收集了用户本人的数据，并且靠网络效应进行病毒式传播，也收集了用户的好友数据。比如一旦张三使用了这个小程序，平台就可以通知好友李四“你的好友张三玩得很嗨，你要不要也试试？”，一个用户可能有几百个好友，通过这些“种子”可以得到更多用户的个人信息。

这些信息一旦被泄露，会被“有心者”进行数据分析，再使用用户喜好的方式渗入社交网络，从而达到改变用户心理，从而达到目的，甚至会变成网络犯罪的信息来源，给人们造成经济损失甚至是生命威胁。“徐玉玉”案便是隐私泄露最为惨痛的教训之一，引起人们对网络数据隐私保护的热切关注。

在发生这一切的时候，社交网站既没有被黑客入侵，也没有所谓的主动“泄露”或是“偷盗”数据，所有的参加者都是心甘情愿地让出他们的行为数据的。但你的数据却被搜集，用作各种途径。因为你想要享受这项服务，于是你毫不犹豫地选择用自己的个人信息作为代价，让自己暴露在

信息泄露的威胁之中。

这种“主动式”泄露个人隐私还会在用户安装 App 时发生。据工信部数据显示，中国移动用户数总规模达约 12.93 亿户。可见，移动 App 多么受到大家的喜爱。但是你知道吗，App 泄露隐私的问题也日益突出，在使用 App 的过程中，你的微信昵称、头像、位置、通讯录、电子邮箱信息、QQ 账号密码，甚至身份证号码、银行账户都“裸奔”在互联网海量“大数据”当中。而这些隐私信息，基本上都是自己在下载安装 App 时“同意授权”的。

这种场景你一定不会感到陌生，在你安装 App 的时候，通常手机会提醒我们授予应用权限，而这些权限多种多样，最常见的就是储存权限、调用摄像头麦克风、获取手机识别码等，而你当然不会一条一条地仔细阅读，而是直接拉到底端，点击“确定”。当然，这种情况并不是只发生在你一个人身上，据中国消费者协会调查结果显示，在安装和使用手机 App 时很少有人阅读应用权限和用户协议或隐私政策，偶尔阅读和从不阅读者居多。总是阅读的占 18.1%，经常阅读的占 8.2%，有时阅读的占 16.4%，偶尔阅读的占 31.2%，从不阅读的占 26.2%。

这时候，有的人可能会感到委屈“我阅不阅读意义大吗？就算我全部都阅读了，并且发现了其中的不妥之处，但是我不授权同意，我就没有办法使用这款 App 啊，我能怎么办呢？”确实，这是很多人在现实生活中遇到的状况，现有的大多数 App 在安装时如果不授权或者同意隐私条款就无法使用该项服务，在上述占比 26.2% 从不阅读应用权限和用户协议或隐私政策的受访者中，选择从不阅读的原因主要是不授权就没法用，只能被迫接受的比例占 61.2%（图 4-4）。

为了给用户提供更好的服务，在安装 App 时运营商获取必要的权限无可厚非，但是很多 App 在安装时请求的权限是提供服务时根本不需要的，但是以“强盗”的方式强制用户同意授权一些信息采集权限。比如读取位置信息是我们手机上很多软件都会获取的权限，像是社交软件的定位

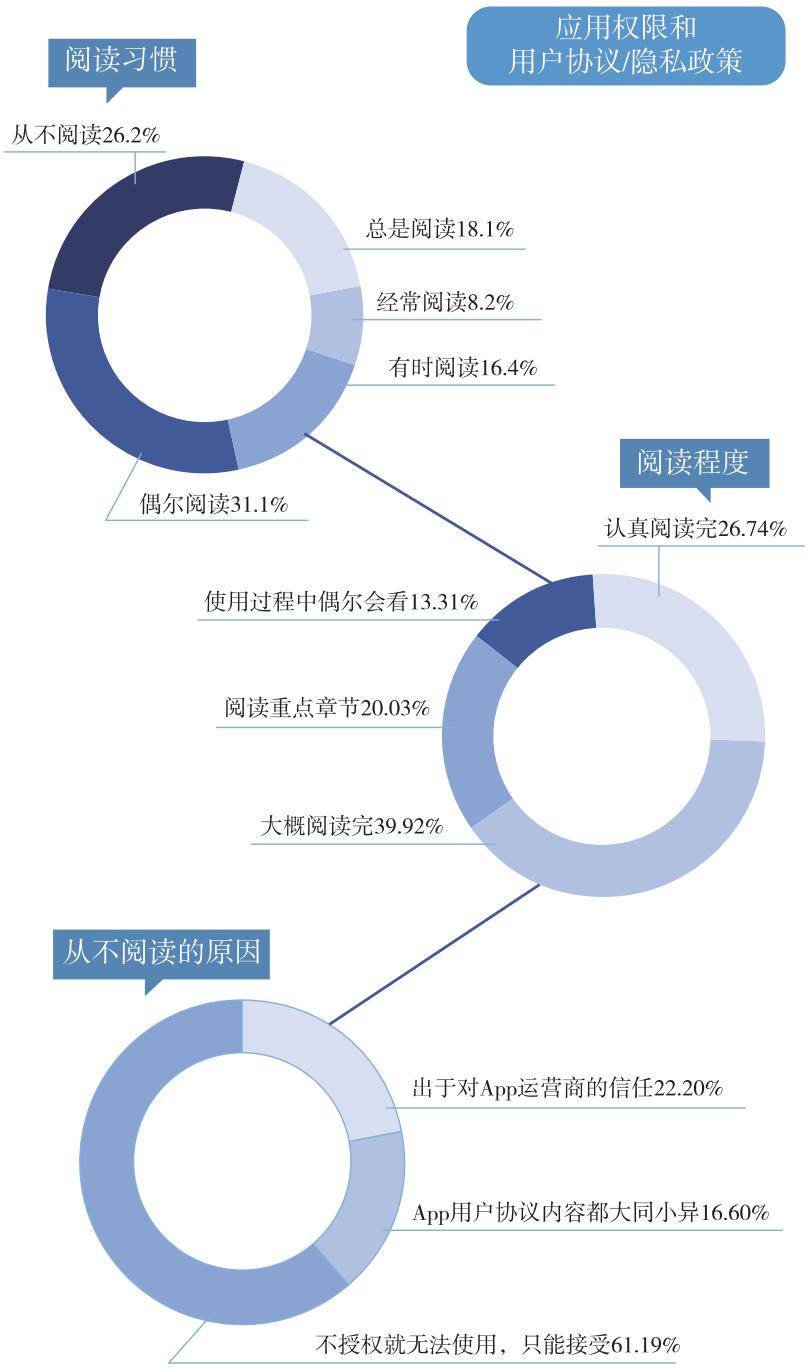

图 4-4　应用权限和隐私协议阅读状况

功能、导航软件、外卖团购软件、新闻客户端等，这些是为了向用户提供服务，这都可以理解。但是有的图像处理软件、电子书软件等一些完全没有社交功能的软件也需要定位的权限，一旦你同意授权使用，你的位置信息就会被非法收集。

运营商读取位置信息权限和访问联系人权限是安装和使用手机 App 时遇到情况最多的，分别占 86.8% 和 62.3%。受访者被要求读取通话记录权限（47.5%）、读取短信记录权限（39.3%）、打开摄像头权限（39.3%）、话筒录音权限（24.6%）的比例也相对较高（图 4-5）。

获取访问权限统计

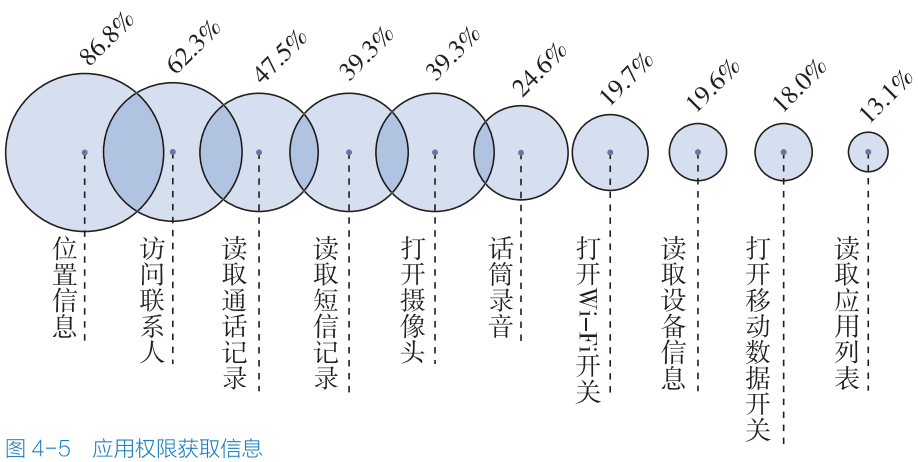

图 4-5　应用权限获取信息

应用权限的滥用是泄露用户隐私的重要原因，国家计算机网络应急技术处理协调中心调研数据显示，国家信息安全漏洞共享平台收录 1710 个涉及移动互联网终端设备或软件产品的漏洞，这都可能成为黑客攻击获取用户信息新的入口。央视《每周质量报告》也曾报道过安卓手机应用在安装时需要开放通信录、地理位置等涉及隐私的权限，严重威胁了用户隐私安全。

中国消费者协会的一系列调查数据也印证了 App 权限滥用是用户隐私信息泄露的重灾区。调查显示，个人信息泄露总体情况比较严重（图 4-6），遇到过个人信息泄露情况的人数占比为 85.2%，没有遇到过个人信息泄露情况的人数占比为 14.8%。

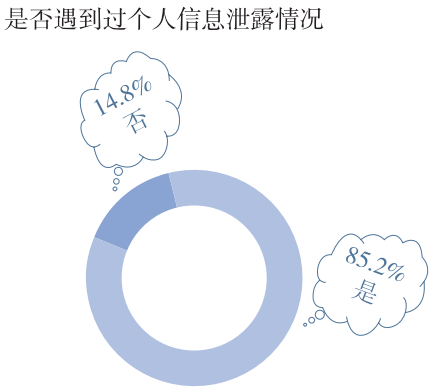

图 4-6　个人信息泄露情况

市民李女士莫名收到某 App 平台发来的催收短信，称其朋友贷款逾期未还，短信中不但公布了其朋友的手机号、身份证号等个人信息，还带有大量恐吓咒骂字眼。发短信的人自称是“借款公司的”，称借款人在借钱时由李女士担保，并且有办法得到李女士的姓名、手机号、身份证号等个人信息，如果借款人不还款，李女士及家人将遭遇厄运。

随后，李女士联系到借款人，说明事由后，对方承认确实从该机构的平台上借了一定数额的钱，但是否认了将李女士填写为担保人，那么为什么借贷平台会向李女士发送催款短信呢？安全专家为我们解答了疑惑，虽然借款人并没有将李女士填为担保人，但是在安装 App 时，应用权限声明条款中要求“手机软件会调取通信录，向有过通话记录的联系人催收短信”，若不同意应用权限要求，则无法使用服务，因此借款人在安装 App 时便授权读取通话信息。如此，便也不难理解为什么借贷平台可以找到李女士。

随后在该 App 使用过程中发现，软件会向用户申请读取手机通信录

的权限，在其《隐私条款》和《用户注册协议》中，也有内容称如逾期未偿还本息，借贷宝可能与第三方共享用户信息等。

无独有偶，市民郭先生近日也收到不少催收公司发来的信息，因自己的一个同学在借款平台上借了钱未按时偿还，催收方就通过同学手机通信录找到了他。不仅收到催款短信，郭先生还接到了许多讨债电话，甚至传说中的“呼死你”也用上了，“响了十几个小时，未接电话得有好几千，但由于号码不同，地域不同，想拦截都拦不住”。

安卓系统手机权限的无限开放和管理缺失，使得众多的软件商任意获取手机用户隐私权限成为了一种普遍现象。随着移动网络竞争愈加激烈，精准营销成为趋势，一些软件开发者即使暂时用不上相关权限，也会获取能够体现手机用户身份、交际特点、活动轨迹等特点的各类隐私信息。因此，权限滥用除了联系人信息、通话记录等隐私内容被窃取之外，手机中的微博、支付钱包等手机应用软件的安装信息也可以被读取，这意味着手机用户的爱好、习惯可以被恶意窃取者通过这些权限摸得一清二楚。特别是一些炒股、金融和支付等软件的账号和密码，如果被恶意监视，则会带来更大的财产损失隐患。

第三节　公共设备漏洞

1. 公共 Wi-Fi

大数据时代，智能设备的功能越来越强大，提供了越来越多的服务，彻底改变了我们对于移动网络的认知，以文字、图片、视频为承载方式的各类信息接踵而至，大大丰富了我们的碎片时间，因此人们对智能设备的

依赖程度逐渐加深。为了能随意地在任意时间地点购物、上网甚至追剧，人们需要选择合适的上网方法，除了运营商提供的数据网络外，Wi-Fi 凭借着网速快、费用低的特点成为大众无线上网的首选，许多店家有时也以免费 Wi-Fi 为卖点吸引顾客。不过虽然能够免费上网很诱人，但是一些公共场所 Wi-Fi（图 4-7）我们真的能够放心用吗？

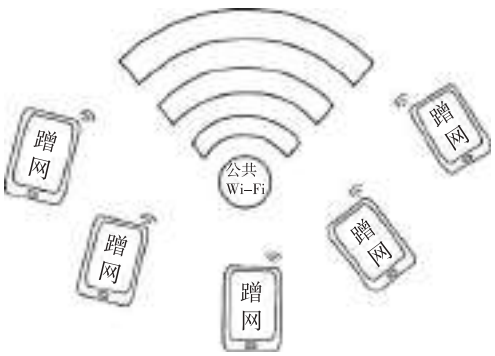

图 4-7　连接免费 Wi-Fi

信息安全组织“雨袭团”为了检测中国一线城市 Wi-Fi 的安全性，曾在北京、上海、广州三地对 68043 个 Wi-Fi 信号进行了调查（包括北京的 23763 个，上海的 26147 个以及广州的 18133 个），包括机场、火车站以及王府井、天安门广场、陆家嘴、天河体育中心、百脑汇电脑城等客流密集地。他们以此发布的《中国一线城市 Wi-Fi 安全与潜在威胁调查报告》显示，有 8.5% 的 Wi-Fi 信号为“钓鱼”Wi-Fi。这些钓鱼 Wi-Fi 不需要进行安全验证就可以免费使用，但是会盗取用户的个人信息和设备信息，进而实施网络诈骗。

在所有的 Wi-Fi 信号中，有 34% 为第三方公司业务、23% 为店铺自建热点、14% 为寄生虫热点、9% 为公共设备、8.5% 为钓鱼 Wi-Fi、7.5% 为家庭热点、4% 为临时热点。值得注意的是，无密码的免费 Wi-Fi 风险较高。

被判定为不安全的 Wi-Fi 信号 93% 存在着获取用户信息和设备信息的情况，87% 存在广告欺诈和产生流量费用，46% 能以钓鱼等方式盗取账号密码，5% 会修改并植入恶意软件。例如，有的 Wi-Fi 登录页面就要求用户输入身份证号码或 QQ 账号和密码。

而在日常生活中，下面的这个场景你是否很熟悉？

在一个公共场合，为了节省手机流量，你开始搜索附近的公共 Wi-Fi，然后惊喜地发现刚好有一个免费的公共 Wi-Fi，于是你开始打开自己常用的社交或消费软件，登录微博看看关注的人的动态，打开淘宝看到心仪的东西使用支付宝买了下来，并顺便查询了一下之前买的东西的物流信息，然后用手机预定了餐厅，并留下了电话，然后你断开 Wi-Fi，结束这次上网浏览。

这看起来什么都没发生？但其实在你使用免费 Wi-Fi 浏览数据的这短短时间内，你的各种信息都完全暴露在不法分子的眼皮之下。当你打开了消费类软件并进行下单后，你的订单和消费记录将统统被提取、传输，包括电话号码、预约时间、下单留的地址、家庭住址、身份证号码、银行卡号，甚至某天某时你看了一场什么电影；如果你进行了支付或者登录，你的用户登录密码和支付密码也将暴露在别人面前，一个人衣食住行的生活习惯等个人隐私，都可能被不法分子一点一点摸透。

小梨是个名副其实的“蹭网族”，外出时第一件事情就是搜索、连接附近免费的公共 Wi-Fi，但是最近她觉得很诡异，似乎自己在网络上成了“透明人”。无论是短信还是微信，总有大量不明来源的推销信息骚扰她，而且这些信息大多还能知道她近期的消费需求，尤其是“双 11”前，推荐的产品大都是她有意向购买的，而她确信自己的手机并没有中毒，因为使用安全软件检测和查杀都没有发现病毒。短信依旧发个不停，微信也频繁有人加她推销产品，无奈之下，小梨换了新的手机，但这并没有解决她苦恼的问题，那些看似精准的推销信息依旧没有消停，让她感到十分不解。

她将上述经历发到朋友圈，没想到有不少好友也在下面纷纷留言，称

062 大数据时代的隐私保护

经常连接免费 Wi-Fi 后，觉得手机似乎“中毒”了，不论是广告还是推销都相当精准，好比读心术，但又不知道哪里出了问题。公共 Wi-Fi 安全人员推测，这种现象可能是因为“蹭网”导致的信息泄露。免费 Wi-Fi 连接的次数太多，个人资料被多个免费 Wi-Fi 的运营机构搜集，经过大数据技术的处理、分类，最后被反复“倒卖”才造成这样的麻烦。

那么这些个人信息究竟是如何被泄露的呢?

最主要的原因是手机上的许多软件并没有按工信部有关规定的要求，对用户隐私信息数据采取必要的保护措施，且公共无线网络的传输加密等级一般都很低，可以被黑客轻易地入侵，甚至有的黑客专门在商场处设置免费 Wi-Fi，引诱人们登录使用，之后从无线路由器传输的数据中提取到用户姓名、出生日期、身份证件号码、住址等个人隐私信息（图 4-8）。因此在面对免费 Wi-Fi 时，大家都应该更加谨慎，要知道每一次不安全的连接和分享，都可能造成自身及他人隐私信息的泄露，甚至还可能对财产和生命安全造成威胁。

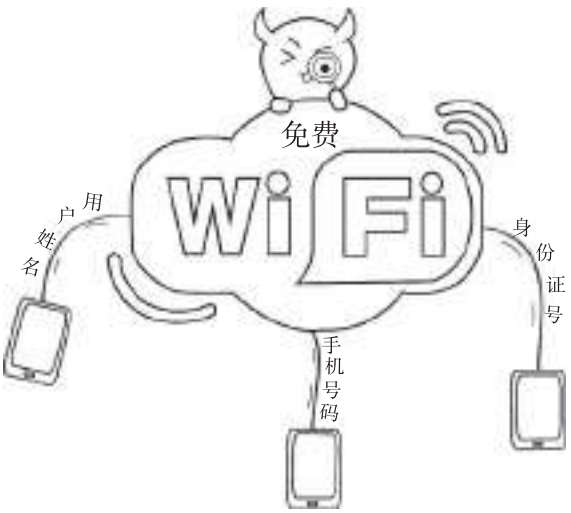

图 4-8　免费 Wi-Fi 获取用户隐私

2. 云端存储

大数据时代，人们对于“云”的概念已经很熟悉了。用户经常会遇到手机或电脑存储空间不足、数据需要存储的时间比设备使用时间长、存储在硬盘的数据可能丢失等烦恼，云端数据储存的出现在一定程度上解决了这个问题，储存在云端的数据不仅可以长时间保存，不被丢失，还能为用户节约出设备的储存空间，受到广大用户的喜爱。比如，有很多用户喜欢随时将自己用手机或平板拍摄的照片与视频，甚至通信录、办公文件等通过云存储快速上传到网盘中储存或者备份，这样可以非常快捷地通过WEB 或 PC 客户端在异地即时取回。不仅是个人，甚至一些企业也将各种数据上传存储至云端。

但是你知道吗？如果你没有使用隐私保护软件，将隐私视频、图片等文件进行加密处理后再放置云端，你上传的每一张照片或其他文件都有可能以明文形式保存在云存储的服务端，一旦网站被黑客攻破，这些内容可以被黑客直接获取。一些平台的管理员甚至可以直接查看和删除用户上传的文件，这些文件中不乏用户的机密文件或者隐私文件，资料在云端的储存安全与用户的隐私将会是一个最大的隐忧。

身边朋友是不是经常会遇到这样的场景，无意间误删除手机上的相册，并且是和家人旅游，具有珍藏价值的相册，扼腕叹息，无可奈何；或者是一不小心丢了手机，虽然土豪认为手机不值钱，但手机中的通信录、文件等资料却十分有价值，还有手机不小心丢进洗衣机损坏的，诸如此类的意外导致手机里的数据丢失的事件多不胜数。最好的解决办法就是定期将重要的数据备份保存，但是很多时候会面临这样的困境，定期保存数据太麻烦，而且大多数人容易忘记。这个时候，百度网盘的“手机备份”功能就显得十分“贴心”了，自动备份相册、通信录、短信等重要资料，避免了手机出故障或丢失后的数据无法找回的尴尬，并且百度网盘的大部分功能都是免费开放使用的。因此，大家在资料储存或者存放隐私文件的时

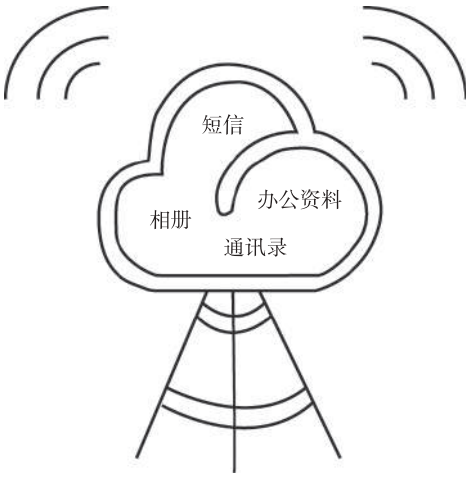

图 4-9　存储在云端的隐私信息

候都会用到百度网盘（图 4-9）。

但是在使用百度网盘分享功能的时候，一定要小心谨慎，不然很容易就会中招，陷入隐私泄露的危机中。曾经沸沸扬扬的百度网盘用户隐私数据泄露风波，泄露隐私信息的人数达到千万级别，罪魁祸首就是用户使用了公开“分享”功能。用户一旦使用公开“分享”功能，任何人都可以通过第三方网站轻易搜索、查看、下载大量公开分享在网盘上的通信录、办公资料甚至护照图片、银行卡图片等个人私密文件，甚至连公司、高校、政府内部文件等隐私内容也可看到。

储存在云端的隐私泄露事件层出不穷，iCloud 是苹果公司提供的云端服务，使用者可以免费存储资料，并且可以同步备份邮件、照片、联系人、日历等资料。这一功能给广大苹果用户带来便利，但同时，也可能将他们拉入隐私泄露的旋涡中。据媒体报道，有用户公开发布了众多女星隐私照片，这些照片在网络上被疯狂传播和下载，引发了社会对云端数据安全的广泛关注。

令人难以置信的是，这些照片是黑客攻击了苹果的多个 iCloud 账号之后流出的，有些照片甚至是当事人在很久以前就删除的照片。黑客在网络中尽可能多地收集她们的信息，如电子邮箱、出生日期等信息，然后根据这些信息不断猜测用户的账号密码，直至最终成功登录其账号，获取想要的信息。更糟糕的是，因为很多苹果用户都注册拥有了 Apple ID，并且绑定了信用卡信息，而大部分用户的 iCloud 账号和这个 ID 账号是相同的，一旦账号被攻破，外泄的除了照片外，还有用户的信用卡信息。

数据储存在云端确实为我们的生活带来很多的便利，但如果用户的移动终端或客户端用户名和密码泄露或被非法窃取，服务器上用户的隐私数据安全将难以保证。这意味着，用户上传到云上的资料信息越多、个人隐私越多，信息安全隐患就越大。

第四节　恶意程序

恶意程序是威胁隐私安全的重大因素之一，最常见的表现形式是病毒和木马。前者往往具有一定的破坏性，更像是打砸抢烧的强盗，后者倾向于偷偷窃取，更像是暗中出手的小偷。

1. 病毒程序

在智能手机普及的今天，我们用智能手机连接世界，世界也通过手机连接我们，任何人都有可能窥视我们的隐私，在智能手机裸奔的世界里，任何不经意的小举动都是泄露隐私的途径。日常生活中，手机中的短信垃圾、房产中介等骚扰电话和带病毒的诈骗信息如雪花般纷至沓来，尤其是手机病毒，在不经意间就潜伏在你的手机上，盗取手机上的个人通信录、日程安排、个人身份信息等隐私信息，甚至连银行卡的存款只有两位数这样的秘密也可能会被知道。

大数据时代，新的计算机病毒层出不穷，旧的病毒也没有就此消亡，而是不断发展，呈现出多样化的趋势，影响我们的学习和生活，给隐私保护带来极大的挑战。那么你对计算机病毒的了解有多少呢？一起来了解一下计算机病毒吧！

计算机病毒已经出现很多年了。早在 1949 年，计算机科学刚刚开始

的时候，计算机之父冯·诺依曼就声称，可以自我复制的程序并非天方夜谭，这是最早提出病毒的概念。在如今，计算机病毒的概念不断延伸，已经扩大为指能够对计算机软件、硬件或数据进行破坏的计算机程序，除了破坏性，病毒还普遍具有一定的传染性和自我复制性，这也是病毒可以通过网络大规模传播的原因之一。

从 1949 年出现病毒的概念到如今病毒不断地变种发展成为威胁隐私保护的重要因素，先后出现了很多影响力十分重大的计算机病毒，下面介绍一些影响大、有代表性和历史性的病毒。

（1）大脑病毒

大脑病毒是世界上公认的第一个流行的计算机病毒，它是由一对巴基斯坦兄弟在 1986 年编写的。这对兄弟所在公司出售的软件经常被非法复制，使得购买正版软件的人越来越少。为了防止他们的软件被任意盗拷，兄弟俩编写了大脑病毒来追踪和攻击非法使用其公司软件的人，只要有人盗拷他们的软件，大脑病毒会将盗用者硬盘的剩余空间“吃掉”。所以说，人类历史上第一款病毒是为了“正义”目的而编写的“错误”程序。

（2）莫里斯蠕虫

如果说之前的大脑病毒是为了防止软件盗拷而设计的病毒，只能通过数据的拷贝传播，还不具备大规模自动感染的能力，那么“莫里斯蠕虫”的出现，彻底结束了这个时代，使得病毒通过互联网扩散成为现实。

莫里斯蠕虫由康奈尔大学的罗特·莫里斯在 1988 年制作，他编写该病毒的初衷并不是为了破坏，而是想利用蠕虫自我复制的特性测试网络规模，向人们证明网络漏洞的存在，但是病毒扩散的影响很快就超出了他的控制范围。国家航空和航天局、军事基地和主要大学的计算机网络均遭受莫里斯蠕虫的攻击，致使网络中 6000 多台计算机被感染，这大概占当时连入网络计算机数量的十分之一，直接经济损失高达 9600 万美元。莫里斯也因此被判处有期徒刑 3 年、1 万美元罚款和 400 小时的社区服务。之

后出现的各类蠕虫病毒都或多或少模仿了莫里斯蠕虫。

到目前为止，蠕虫都还是常见的计算机病毒之一，它是利用网络进行复制和传播的一种病毒。其最初被命名为蠕虫的原因是在 DOS 环境下，病毒发作时会在屏幕上出现一条类似虫子的东西，胡乱吃掉屏幕上的字母并将其改形。

（3）冲击波病毒

2003 年 8 月，冲击波病毒席卷全球，它利用 RPC 漏洞进行传播，RPC 是微软网络接口，是操作系统的一种消息传递功能。该病毒感染速度极快，一周内感染了全球约 80% 的计算机，尤其是未对 RPC 漏洞打补丁的计算机。被感染的计算机，操作系统不断报告“PRC 意外终止，系统即将重新启动”（图 4-10），除此之外，许多依赖 RPC 服务的功能也出现问题，比如不能进行复制、粘贴，无法查看网络属性等。冲击波病毒是历史上影响最大的病毒，向人们展示了计算机不打补丁的危险性有多高。

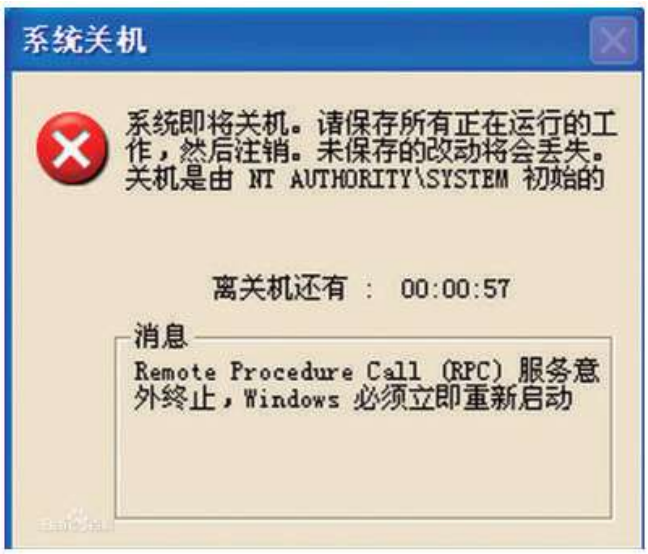

图 4-10　冲击波病毒

（4）熊猫烧香

从2006年年底到2007年年初，短短的两个多月时间，一个名为“熊猫烧香”的病毒不断入侵个人电脑、感染门户网站、击溃数据系统，给上百万个人用户、网吧及企业局域网用户带来无法估量的损失，被《2006年度中国大陆地区电脑病毒疫情和互联网安全报告》评为“毒王”，一举使得“熊猫烧香”成为历史上知名度最高的一个“国产”病毒。

“熊猫烧香”是一款拥有自动传播、自动感染硬盘能力和强大的破坏能力的病毒，感染该病毒的计算机中所有的可执行程序的图标都被改为熊猫举着三根香的图片（图4-11），并且会出现蓝屏、频繁重启以及系统中数据被破坏，导致计算机系统甚至整个局域网瘫痪。

图4-11 熊猫烧香病毒

（5）震网病毒

震网病毒是第一个针对工业系统的计算机病毒，也被认为是世界上首个网络“超级破坏性武器”，计算机安防专家认为，该病毒是有史以来最高端的蠕虫病毒。全球感染的超过45000个工业控制系统中，近60%出

现在伊朗，伊朗核设施遭受震网病毒攻击，大量生产核燃料的离心机被破坏。

（6）勒索病毒

勒索病毒是一种新型电脑病毒，主要以邮件为传播方式。勒索病毒文件一般以附件的发送给受害者。一旦被用户点击打开，病毒就会将本地 Office 文档、图片等文件进行格式篡改和加密；加密完成后，还会在桌面等明显位置生成勒索提示文件，指导用户去缴纳赎金。这种病毒利用各种加密算法对文件进行加密，被感染者一般无法解密，任何杀毒软件都无法解密勒索病毒加密的文件，受害者只有缴纳赎金拿到解密的私钥才有可能破解。该类型病毒可以导致重要文件无法读取，关键数据被损坏，给用户的正常工作带来了极为严重的影响。

近年来，各类敲诈勒索软件在我国大量涌现、肆虐传播，成为近两年增长最快的网络威胁之一。永恒之蓝勒索蠕虫是最为人们所熟知的一款勒索病毒，它的英文名称为 WannaCry，既是一款勒索软件，又是一款蠕虫病毒，同时还采用了军用攻击武器“永恒之蓝”，其感染计算机后，会将计算机中的办公文档、照片、视频等文件加密，向用户勒索比特币。

虽然，WannaCry 敲诈勒索病毒是最活跃、影响最大的病毒，但也仅在敲诈类病毒总量中排第四，最多的是带有感染传播方式的 PolyRansom。WannaCry 由于使用了 Windows 系统漏洞进行传播，因此范围波及全球。后续的 Petya 新型勒索病毒的敲诈手段与 WannaCry 相似，但更具有破坏性，直接加密了用户的硬盘数据，导致用户无法进入 Windows 系统。下面简单介绍这几种勒索病毒。

PolyRansom 勒索病毒。PolyRansom 是一种感染式病毒家族，它能够通过覆盖原始文件来修改文件自身。它把原始文件修改成可执行文件，并附加病毒，就像一个生物一样，具有自我繁殖、变异、互相传染的能力，每个都不一样。PolyRansom 运行后会拷贝自身到多个目录下，将自身注册为系统服务，使自身随开机启动，搜索并感染用户的重要文件，

将原文件以加密的形式保存在新建文件夹下，在锁定计算机后，就会弹出勒索窗口，让用户支付金钱（图 4-12）。同时病毒还会篡改开机密码，使用户无法进入计算机。

图 4-12　PolyRansom 勒索病毒

WannaCry 勒索病毒。WannaCry 是一种新型勒索病毒软件，利用美国国家安全局泄露的危险漏洞“永恒之蓝”进行传播，用户无须进行任何操作，只要开机联网，计算机就有可能被感染。被该勒索软件入侵后，用户主机系统内的照片、图片、文档、音频、视频等几乎所有类型的文件都将被加密，加密文件的后缀名被统一修改为 .WNCRY，受害者电脑被锁定，并会在桌面弹出勒索对话框，要求受害者支付解密赎金（图 4-13）。

Petya 勒索病毒。Petya 是一种类似于 WannaCry 的变体勒索病毒软件，它的破坏性比传统的勒索软件更大。它利用“永恒之蓝”和“永恒浪漫”两个漏洞传播。用户一旦感染，病毒会修改系统硬盘的数据，将硬盘整个加密和锁死，当电脑重启时，病毒会在 Windows 操作系统之前接

管电脑，执行加密等恶意操作。此外，如果一台受感染计算机拥有网络的管理员权限，那么这个网络中的所有电脑都会被感染。受到感染的计算机用户被要求支付 300 美元才能解锁（图 4-14）。

图 4-13　WannaCry 勒索病毒

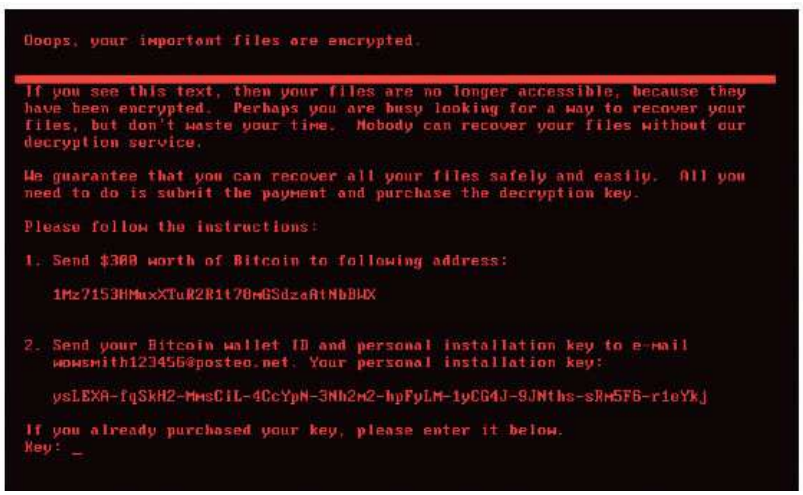

图 4-14　Petya 勒索病毒

勒索病毒事件频繁爆发，不仅造成了巨大经济损失，还威胁到人们日常的工作、生活。网络攻击目标从政府机构扩大到民众社会生活各个方面，涉及电信、金融、能源等多个领域。那么，勒索病毒有什么特点，又会给我们带来哪些危害呢？

传播速度快。勒索软件和很多新技术结合，借助网络传播，一旦电脑连接网络，用户甚至不需要任何操作，勒索病毒就可能利用漏洞感染计算机，传播速度非常快，在重灾区国家，新病毒变种的传播速度达到每 10 分钟感染 5000 余台电脑，多家运营商、石油公司、零售商、机场、ATM 机等企业和公共设施已大量沦陷。

危害范围大。2017 年 5 月 12 日，WannaCry 勒索病毒突然爆发，超过 150 个国家至少 30 万名用户中招。在 WannaCry 爆发的一天之内，该勒索蠕虫已经攻击了全球近百个国家的超过 10 万家企业和公共组织，其中包括 1600 家美国组织，11200 家俄罗斯组织。国内被感染的组织和机构已经覆盖了几乎所有地区，影响范围遍布高校、火车站、自助终端、邮政、加油站、医院、政府办事终端等多个领域。

文件损失。勒索病毒主要是危害电脑数据安全，对于硬盘上有重要数据的用户来说，一旦电脑中勒索病毒，可能会导致数据丢失，而一些重要数据是无价的，一旦被损坏或者丢失，价值是无可估量的。比如 WannaCry 勒索病毒危害全球上百个国家，机场、车站、地铁、医院、电信公司、公安等诸多社会基础设施中的无数宝贵资料被病毒加密，甚至有大学生毕业论文被锁死，可谓损失惨重。

经济损失严重。勒索病毒传播速度快、影响范围大，电脑感染勒索病毒后所造成的经济损失，除了不法分子索要比特币赎金外，还包括被锁定甚至丢失的文件带来的经济效益。之前爆发的 WannaCry 勒索病毒席卷全球，造成损失达 550 亿元。

2. 木马程序

大数据时代，除了破坏计算机资料的病毒外，更让人担心的莫过于木马程序了。木马是目前比较流行的恶意程序，它可以非法控制计算机，或者是在他人计算机中从事秘密恶意活动。比如秘密潜伏在被控设备中，盗窃被控用户的数据或者是个人隐私信息，从而获取一定的经济利益。

与传统的病毒不同，木马程序一般不会自我繁殖，也不会“刻意”地去感染其他文件或者破坏系统。它通过伪装成合法程序去吸引用户下载执行，一旦木马感染成功，木马的控制者就可以在受害者的计算机上进行各种恶意操作，比如秘密操控、文件窃取、强弹窗广告，甚至可以远程操控被感染的主机。

木马病毒的产生和广泛扩散，可以在用户不知不觉中盗取用户的隐私信息，比如网站的账号和密码，严重威胁了用户的隐私安全。下面简单介绍两种窃取用户隐私信息的常见木马程序。

（1）盗号木马

盗号木马是最早流行的木马程序，它可以通过监控用户键盘输入、监控软件交互接口、透明窗隐藏覆盖等方式来窃取用户的网络账号和密码，这些网络账号可能包括网银账号、网友账号和社交网络账号。

曾经流行一时的 QQ 粘虫木马就是通过透明窗隐藏覆盖技术来盗号的，那么什么是透明窗隐藏覆盖技术呢？就是当用户打开 QQ 聊天软件时，QQ 粘虫木马会在 QQ 登录窗口的相同位置生成一个相同大小、透明、看不见的窗口，此时，用户以为在 QQ 登录窗口输入的账号和密码，但实际上却是在木马制造的透明窗口中输入的，于是，账号就通过这种方式被盗取了。

木马盗取用户的账号和密码后，一般会通过发送电子邮件或远程提交的方式将盗取的信息发送给木马的操控者。在这个过程中，账号被窃取的受害者一般没有任何感觉。

（2）窃私木马

窃私木马多见于智能终端，它们是专门用来窃取用户隐私信息的。而在隐私窃取类手机恶意程序中，绝大多数都是专门窃取个人信息，包括通信录、短信、通话信息、银行信息、社交软件聊天记录、录音和照片等，严重危害用户的隐私信息安全。

据专业安全机构调查显示，67.4% 的窃私木马会窃取短信信息，34.8% 会窃取用户手机银行信息，10.0% 会窃取手机联系人信息，3.7% 会窃取手机通话记录，2.0% 会窃取社交软件（如微信、QQ 等）聊天记录，1.8% 会窃取手机录音信息，0.1% 会窃取手机中的照片。可以看出，窃私木马窃取短信信息的比例尤其高，其中重要的原因就是不法分子通过这种方式窃取用户的短信验证码信息，这是不法分子使用用户账号、盗刷用户网银的重要方式之一。

在看完上述对木马的介绍，也许有些人会质疑，木马真的有这么厉害吗，我为啥没有发现？下面通过经常发生在我们身边的案例，帮助大家更深切地了解到手机木马的危害程度。

吴先生感到十分纳闷，他绑定手机的两张银行卡中被盗了 8 万元，而他的手机上并没有收到任何的短信消费提示，于是他向警方寻求帮助。办案民警发现，吴先生两张银行卡中被盗刷的 8 万余元都是通过网购，以线上支付的消费方式被盗走。顺着这个线索，警方很快找到犯罪人员林某，经林某交代，他通过木马短信向吴先生的手机中种植了木马病毒，得到吴先生绑定在手机上的银行卡信息，在消费过程中，拦截了发送到手机上的验证码短信和消费提醒短信，因此，即使他在成功盗刷后，林先生也未收到任何的消费提醒短信。

手机木马病毒一般依附常见的游戏和软件应用，具有较强的隐蔽性，不容易被发现。一旦感染受害人的手机后，病毒就会在后台悄悄地自动记录本机所有的短信内容和通话记录，并且会将这些信息上传到指定的服务器，如果短信中有银行账号密码或者其他重要信息，被病毒偷窥后，可能

产生严重的经济、名誉等损失。

木马病毒还可根据服务器返回的指令执行后台拨打电话或者发送短信的指令，在用户毫不知情的情况下肆意消耗用户资费。犯罪分子通过木马病毒获取用户的隐私信息后，可以开通网络支付等转账和消费途径，而手机木马也会拦截受害人手机上的相关验证短信等，并将这些短信转发至指定手机上，随后犯罪分子通过这些验证短信，最终通过网上支付等方式，将受害人的钱款转走。而受害人在这个过程中一直收不到短信，被蒙在鼓里。

此外，木马病毒通过远程控制在后台将用户的手机配置等信息发送到指定服务器，泄露用户隐私；成功获取手机配置信息后，该病毒会通过指令将不明软件远程安装在用户手机中，同时有可能卸载其他干扰该病毒运行的软件，使得用户手机可能处于不设防状态，在后续病毒侵入过程中蒙受更大的损失。

木马病毒一般通过哪些形式传播呢？

（1）社交工具中的链接

在QQ、微信、邮件等各种聊天工具出现之前，手机病毒的传播主要是通过短信，将含有木马病毒的未知链接发送到用户的手机上，但随着各种各样聊天工具的出现，人们的交流方式已经不仅仅限于短信，也通过QQ、微信、邮件等各种聊天工具，这些聊天工具中的一些未知链接也存在安全隐患，一旦点击，极可能导致手机感染木马病毒（图4-15）。

图4-15　存在安全隐患的未知链接

（2）资源下载

木马病毒可以依附在很多常用软件和游戏应用中，占用的内存很小，还有可能伪装成杀毒软件、系统补丁以及小游戏等，而现在网络上有很多资源提供手机下载资源，如果不是正规的应用市场，提供的资源中可能隐藏很多的手机病毒，一旦下载并安装这些资源，病毒也就随之潜伏在手机中（图 4-16）。

图 4-16　不正规资源下载途径

（3）无线传播

蓝牙、红外线 Wi-Fi 等无线技术的普及为手机病毒的广泛传播创造了条件，一些手机病毒通过破解蓝牙匹配密码来实现病毒文件的传播，用户一旦接受病毒文件并点击后，手机就会被病毒感染。

（4）危险网站

随着智能手机功能的强大，人们可以使用手机浏览器来访问很多网

站，但一些网站中隐匿着大量的手机病毒（图 4-17），比如很多的黑客网站、色情网站和中奖网站，一旦浏览了这些网站，手机病毒顺势就隐藏在手机中了。

图 4-17　存在安全隐患的网站

第五节　网站漏洞

大数据技术的发展给我们的生活带来了越来越多的便利，比如使用大数据技术，招聘网站可以迅速帮你找到满意的工作，婚恋网站更好地为你解决婚姻大事等。但是你知道吗？这些网站在带给我们便利的同时，可能存在很大的安全漏洞，这些漏洞很有可能被有心之人利用来获取网站上我们的个人信息，而个人隐私信息一旦被泄露，可能会带给我们生活无尽的烦恼，比如各种诈骗电话、垃圾短信、骚扰电话。

据某安全平台透露，各类网站上的安全漏洞十分严重，涉及居民隐

私、用户密码等隐私的信息超过亿万条，从个人隐私到商业机密，从学历工作到汽车定位，在安全漏洞下，都能被黑客一览无余，隐私信息泄露范围之广，触目惊心。比如某省计生委网站上的漏洞，导致全省 7000 多万居民的隐私数据在黑客眼前“裸奔”，包括居民身份证号、住址，甚至配偶、子女和家庭关系等。再比如，某招聘网站的一个漏洞，可以成功将用户登录邮箱的密码重置。也就是说，只要在此网站上注册过的用户，学历、职业、收入等信息都有可能被泄露。这些隐私数据一旦被获取，在大数据技术的作用下，可以分析出他们的购物喜好、心理意识，给他们打上不同的标签，再根据这些标签来选择这些数据不同的使用方式，极有可能会用作不正当或者犯罪行为，比如假医疗药品的推销，实施各种诈骗。

使用浏览器进行网页浏览一直是普通计算机用户使用网络的常见方式，因此衍生出很多针对浏览器的攻击方法，其中主要的两种方式时网页挂马和钓鱼网站，前者通过将恶意程序植入用户的智能设备默默窃取信息，后者是引诱用户在虚假页面输入自己的隐私信息。现在使用智能设备或者 App 上网成为用户访问网络的主流方式，但是很多 App 中都会内嵌浏览器模块，可以打开网址链接以浏览网页，给用户的隐私信息带来了极大的安全威胁。

网页挂马是指在网页中写入一段恶意代码，当用户使用有漏洞的浏览器浏览挂马网页时，这段恶意代码就会在用户的计算机或者手机中运行，导致计算机或者手机感染病毒或者木马，用户对感染病毒的过程没有任何的察觉，由于挂马是利用浏览器漏洞进行的，这大大降低了网页挂马的难度，因此，在网页挂马最活跃的时期，每天最多可能出现数千至上万个挂马网页，使很多用户深受其害。

搭建“钓鱼网站”是另一种网站漏洞利用的常见方式，钓鱼网站是通过各种非法手段，比如漏洞利用、伪造网页等，对真实网站的地址以及页面内容进行冒充，用来诱骗用户填写银行卡、身份信息等信息或者模仿银行在线支付、电子交易网站，骗取用户的银行卡信息或者在线支付账号密

码。常见的钓鱼网站包括：虚假购物网站、仿冒银行网站、虚假中奖网站和虚假 QQ 空间等。用户一旦在钓鱼界面填写自己的信息，钓鱼网站会将用户的信息发送到指定服务器，不法分子就可以搜集到用户的大量隐私数据，比如银行账户、密码、信用卡、账户等数据，这些数据被不法分子贩卖或者用作诈骗行为。

“钓鱼网站”的危害非常大，因为它伪装成各种正常行为来实施不法行为，比如正规网站的登录、退款或者好久不见的老友邮件（图 4-18），人们对这些行为的防范意识会小很多，这样不法分子搜集到用户隐私信息或者达到其他不法目的概率就大很多。如果你对钓鱼网站危害的理解还没有那么深入的话，下面的例子会让你意识到钓鱼网站的可怕之处。

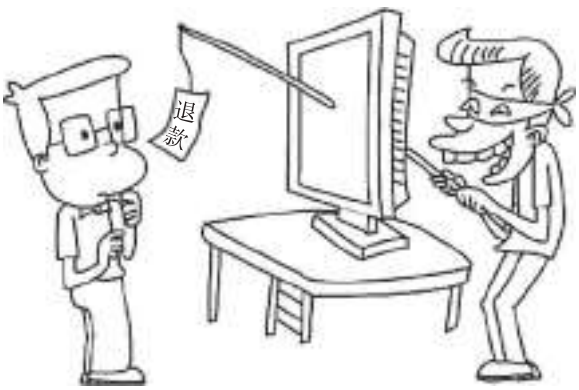

图 4-18　钓鱼网站

许先生在常用的购物网站购买了一件运动背心，两天后，他接到了一个自称是客服的电话，对方准确地说出了他下单的时间、个人信息、购买的物品信息、价格等，并告诉他说因为他是晚上下的单，网站在做维护，导致下单失败，还让他查询是不是没有商品的物流信息，上网站查询了自己的购物信息，发现所购商品的物流信息为空，这时的许先生深信对方正是客服。

接下来，对方称为许先生办理退款，并发给他一个网站，打开后的退

款网页看起来没有任何问题，需要用户按照选项填写退款银行、持卡人姓名、证件、银行卡号、预留手机等，最后是验证码，许先生一一填写后，点击了“确认退款”。不一会儿，他的手机就收到扣款信息，被扣款 3900 元。此时的许先生才恍然大悟，反应过来对方是骗子。以相同方式被骗的用户不在少数，被骗金额最多的高达 12 万元。

退款网站是一种最常用的钓鱼网站，被骗的用户对常用的购物网站比较熟悉，而对一些进行退单、退款操作的网址却不太了解，很难分辨网址的真假，不法分子通过伪造一个无论从内容上还是形式上都与正规退款网站极为相似的网站，获取用户的个人敏感信息，如姓名、公司的职位、邮箱、银行账户等重要隐私信息，在信息收集的过程中，用户基本不会察觉到自己的隐私信息正在被泄露，只有不法分子在获取隐私信息后再实施其他动作后，比如诈骗、窃取文件等，用户才会意识到自己被“钓鱼”了。

不法分子通过钓鱼网站等特殊渠道得到用户的隐私信息，进行定向诈骗，甚至利用盗取的身份证等信息办理信用卡，用于套利、伪造虚假身份等不法活动。除了定向诈骗，更有黑客将各种信息分门别类卖给不同的商家，例如将患者信息卖给医院或卖药的商家，甚至给卖假药的，用来做精准营销。曾有机构统计，每年定向诈骗产生的经济损失高达数亿元。这种诈骗手段，由于不法分子掌握了真实的个人信息，成功率非常高。

此外，由于钓鱼网站的实质是内容的欺骗，而页面本身一般并不包含任何恶意代码，没有代码层面的恶意特征，甚至在很多情况下，即使是专业安全人员，也很难仅从页面内来判断网页内容的真实性，因此，尽管从制作技术上来说，钓鱼网站要比网页挂马简单得多，但是它的识别难度更大。

第五章

大数据时代下如何保护隐私？

在生活中，你肯定遇到下面这样的情况：刚刚买了房，装修公司的电话就打过来了；孩子刚到上学年龄，培训机构的邀请电话就来了；网上购物刚下订单，无货退款的诈骗电话就跟来了；预订航班还没起飞，退票改签的诈骗电话就会紧随而至……

这些骚扰电话烦不胜烦，有时我们还会被这些电话欺骗，经济上遭受一定损失。归根究底，这是因为我们的个人隐私信息遭到了泄露，于是如何让自己使用互联网，而不是让互联网“使用”自己成为目前最紧要的问题。本章将针对第四章提出的五类隐私泄露的途径，分别从自身如何提高隐私意识，科研人员在技术层面做出了什么努力，行业社会如何提高自身规范以及国家在法律法规方面给予了什么支持四方面，分析在大数据时代下保护个人隐私的方法，并且介绍了国际隐私保护经验和隐私泄露后如何降低损失，以供大家参考。

第一节 个人主动保护

与传统隐私泄露不同，大数据时代下，公民隐私信息泄露的途径都源于日常生活。受我国历史文化和传统观念的影响，中国人的观念中对于隐私权的认识不全面、不深刻，重视程度不够，对个人的隐私信息缺乏的正确认识，致使在现代环境中的隐私法律保护意识薄弱。

尽管近年来社会的进步发展，保护个人隐私的法律意识已经得到提升，意识到个人资料信息的保护、归属和使用权限，但是与国外相比仍有较大的差距。由于缺少相关的法律条文，人们在上网时的自我保护依旧存在问题，例如盲目相信网上的隐私保护条款，进而留下自己的电话、姓名、账号等资料信息，为自己隐私的保护留下了隐患，并且在隐私受到侵害时选择沉默而不是采取法律途径。

未来，大数据技术将在更多的行业领域应用，为了更好地保护个人隐私不被泄露，与其被动等待别人保护自己，不如主动出击，从自身做起，提高自身隐私保护意识，养成良好的使用网络的习惯，为自己在大数据时代争取一席安全之地。

1. 谨慎使用隐私信息

在日常使用互联网的过程中，我们可能都会无意识地暴露名字、位置等隐私信息。下面给出了一些简单实用的建议：

（1）通过正规渠道网购

之前发生过不少消费者在网上购买过商品后，就有骗子假装是卖家，说消费者所购买的商品没货了，为了商家在网购平台上的信誉，需要在另

一个软件上退款，之后就会发链接或者二维码给消费者，一旦点开链接下载了链接中的内容，消费者的手机中就可能被植入木马盗取钱财。因此在与卖家交谈时，需要谨慎确认卖家的身份，不要随便点击商家发送的链接，最好从正常渠道支付或退款；不要轻易接收和安装网页要求下载的不明软件；慎重填写银行账户和密码，防止密码泄露造成经济损失。

此外，还有些黑客通过构造一个与原购物网站十分相似的新网站欺骗消费者，这样用户在通过网络支付时，支付的钱就会按照黑客预先设置好的路径进了他们的钱包。因此在网购时，注意要仔细核实网站的网址是否正确，以防钓鱼网站。

除此之外，在填写收货地址时，也最好不要填自己家里的具体地址（图 5-1），可邮寄至公司或家附近的代收点，如果必须要写居住地址时，可以只写至楼层，而不具体到房号。收件人的姓名处最好不用真名。

（2）社交网站谨慎回复

社交网站是我们记录生活，拉近与朋友距离的好方式。但在微信、微博、QQ、贴吧等社交网站发表言论，并与别人回复互动的过程中，应注意尽量不要在发表或回复的内容中涉及名字、电话等个人信息，因为这些回复是所有人都能看到的，如有必要可以私聊。此外在存在陌生人的群聊中，也应当尽量避免透露出自己或别人的姓名、职务、工作单位等真实身份信息，以免被有心人收集利用。

此外，在分享照片时更需要注意，因为通过你发的照片，黑客就可以轻松确定你的地理位置信息；还有些家长在朋友圈晒孩子照片时，暴露出了孩子的姓名、就读学校、所住小区；有些人喜欢晒火车票、登机牌，却忘了将姓名、身份证号、二维码等进行模糊处理。

此外，微信中“附近的人”这个设置，也经常被利用来查看他人的照片，因为如果你的朋友圈设置的是陌生人可以查看十张照片，就有足够的隐私暴露在陌生人的面前了，因此最好在微信中将陌生人查看照片的权限关掉，或在发表动态时设置好分组查看。

（3）注册网站少填信息

各类网站制作教程的出现使得很多人仅经过简单学习就能掌握制作网站的方法，各类小型网站层出不穷，一些小网站可能会贩卖注册用户的信息。因此在注册网站时，尽量避免注册小型的或主页信息纷杂的网站，这种网站大多不注重对用户注册的信息保护，用户资料很容易被盗取。

另外在填写网站注册信息时，尽量少填非必填项，如果是必填项，最好不要填写真实姓名、身份证号码、手机号码、家庭住址、兴趣爱好等（图 5-3）。

（4）妥善处置各类单据

在火车票实名制、微博实名制的今天，大多数快递单、车票、购物小票中都包含着网购者的姓名、电话、住址等个人信息；车票、机票上印有购票者姓名、身份证号；购物小票上也包含部分姓名、银行卡号、消费记录等信息。如果随意丢弃这些单据，可能会被不法分子收集利用，导致个人信息泄露。

因此对于已经废弃的含有隐私信息的单据资料，不要随意乱丢，应将单据上的个人信息去除后再丢弃。可以将包裹上带有个人信息的快递单撕碎，或是用刀子或笔将个人信息划掉或涂抹掉。若有的单据比较难撕，可以把风油精等含有醇类物质的液体涂抹到上面，使得字迹可以完全被擦除。

（5）简历填写简洁概要

随着各类找工作网站的盛行，越来越多的人通过网上投简历的方式找工作。大部分简历中都需要填写申请者的姓名、家庭住址、学历信息、工作经验，有的甚至需要家庭关系说明、身份证号等。但需要小心的是，你精心填写的包含着详细的个人信息的简历，可能在被投递到公司之后就被中介网站甚至公司流传到网上，成为不法分子贩卖的数据中的一部分。

因此，在填写简历时需要注意，只将有必要的部分简略填入，不要过于详细地填写本人具体信息，尤其是家庭住址、身份证号等。此外在投递

简历时，还要注意查询一下这些公司是否是正规运营的公司，不要盲目乱投，因为有些人通过注册一个虚假的公司，发布优厚的工资待遇以骗取各种简历信息。

（6）避免小程序获取信息

随着微信小程序的风靡，朋友圈被测测你是什么样的人、看看你是左脑还是右脑发达一类的小程序刷屏，这些小程序看起来没有什么危险，但在进入小程序的时候每个人都被要求点击“允许使用我的用户信息”，不然你就没法参与使用。一些小程序只是使用简单的用户微信头像和微信名称，但是有的还可能会要求调用你的通信录、短信、位置等隐私信息，并且大多数的用户在退出时，并不会想起关掉该程序的隐私权限。

因此，建议一旦用户不再打算使用小程序时，就将小程序中“使用我的用户信息”关闭掉。一种简单的方法是直接下拉微信首页，长按小程序选择删除即可。另一种方法较为复杂，具体操作步骤如下：将微信切换到“发现”页面后，点击最下方的“小程序”按钮。进入小程序页面后，找到我们不打算再使用的小程序。点击“关于 × × × 小程序”的按钮跳转进入该小程序页面后，再点击右上角的“…”菜单按钮，点击“用户信息”后面的白色滚珠按钮，将其关闭掉即可。

此外，使用小程序时可以多注意开发的团队，尽量选择信誉可靠的团队开发的小程序。

（7）仔细分辨免费 Wi-Fi

随着移动互联网的兴起，人们几乎时时处处都需要使用手机，由于使用运营商流量都是需要支付一定费用的，很多人选择连接公共场所的 Wi-Fi。但是，公共场所 Wi-Fi 的安全防护功能一般都比较薄弱，黑客只需凭借一些简单设备，就可截取 Wi-Fi 中传输的数据。

因此，在需要使用无线 Wi-Fi 登录网银或者支付宝时，最好通过专门的 App 客户端访问。另外，在连接 Wi-Fi 时，最好选择官方的，比如机场或者火车站的 Wi-Fi，仔细辨别名称，避免接入不法分子特意设置的

名字相似的网络。最后，为了保护自己的个人信息，最好把 Wi-Fi 连接设置为手动。

2. 设置复杂度高的密码

近年来，智能手机、可穿戴设备、智能摄像头等终端设备迅速发展，给人们的生活带来了便利。我们的日常生活中离不开各种密码，从线下到线上各种支付手段都需要使用密码。邮箱、微信、QQ 等常用的通信手段也是需要使用密码登录。

但由于网民安全意识薄弱，常常使用初始密码等弱口令进行登录，致使智能设备存在被黑客攻击的安全风险隐患。不少不法分子在利益的驱使下，会对存在的网络漏洞进行攻击，以获取大量个人生活影像、照片等个人信息，严重侵犯了公民个人隐私。设置一个相对安全的密码可以很大程度降低隐私泄露的风险，那么应该如何设置一个安全程度较高的密码呢？

也许很多人认为“我把密码设置的很长，这样就够复杂了吧。”但是密码并不是越长就越安全的，为了让人们认识到现有的不良的密码设置习惯，首先我们来了解一下不安全的密码的常见特征：

（1）仅使用英文字母、数字、特殊字符中的其中一种。如 123456、password、iloveyou 等。

（2）使用和用户名相关的信息。比如用户名是 carry770815，使用用户名中的一部分 770815 作为密码。

（3）使用和用户自己相关的信息。比如用户是张三，密码就是张三的姓名、生日、手机号、女朋友的生日、喜欢的歌星名字、单位名称等。

（4）用户喜欢的体育运动。如 basketball、football 等。

（5）密码和用户的电话、传真、手机、邮编、邮箱等联系方式中的任意一个一致。

（6）密码用连续的数字或字母，或同一个字母或者数字，如

3456789、987654、abcdef、88888888、aaaaaa。

综上所述，下面总结了一些密码设置规则，当我们在设置密码时，可以参考下面的一条或几条规则使自己的密码更复杂，账户安全程度更高：

（1）密码长度最好为 6 到 16 个字符，不要太短也不需要太长。

（2）使用英文字母 + 数字 + 特殊字符的组合。比如 sd8bjh*dh、sge352%ds。

（3）先设置基础密码，然后使用统一的规则叠加组合成不同的强密码。比如自己喜欢的单词 + 喜欢的数字排列 + 网站名称的前三个字母或者后三个字母，则淘宝（Taobao）登录密码可以是 Flower100TAO 或者是 Gold520Bao。

（4）定期更换密码：再复杂的密码，一旦用的时间久了，就有很大的可能性泄露，因此最好定期更换密码。

（5）使用密码管理软件。日常生活里各处都需要用户名和密码，很多人抱怨说密码都记不清，不过一般不建议使用简单的 txt 文档记录密码，因为这样很容易遗漏或被他人看到，可以选择采用专业安全的密码管理软件记录密码。

（6）不要到处乱贴自己的密码。有时在工作中由于密码难记，就写在便笺上，贴在座位或者显示器附近提醒自己，但这种行为虽然方便了自己，但也往往方便了陌生人。

（7）不要在公共场合大声说出密码。比如在电梯里、公交车上打电话时，切勿在电话里大声透露自己的密码。

（8）不要多处使用同一个密码。不要在工作场合和生活场合使用同一套密码，重要系统（比如 QQ、网银、12306 等和隐私密切相关的）和非重要系统（一些小的论坛、查阅为主的资料）的密码要分开。

（9）重要系统不要只用密码认证。如大家在登录网上银行的时候，可能还需要结合短信验证码、使用手机 App 扫描等多种手段。

3. 个人电脑安全防护

很多人将大量的个人资料和文件存在个人电脑里，比如家人一起出去玩的照片、个人的身份证扫描件、个人简历、备份的通信录等。个人电脑的普及虽然极大方便了我们的生活，但是也很容易导致隐私泄露，如果电脑被感染病毒、植入木马，则电脑中的许多文件都有随时被黑客盗走的风险，那么我们应该如何保护自己电脑的安全呢?

（1）设置 Administrator 账户密码

Administrator 账户就是我们常说的管理员账户，你在使用电脑时，应该见过下图所示的这种盾牌样子的小图标，带有这种图标的操作就是只有管理员账户才可以执行的操作，简单来说，管理员账户拥有最高电脑管理权限。因此在我们创建管理员账户之后，一定要设置开机口令，且这个口令设置不能过于简单，因为一旦黑客获得我们电脑管理员口令，就能获取更改电脑的所有权限，获取所有他想获得的隐私信息（图 5-1）。

图 5-1　管理计算机密码

设置 Administrator 密码需在安全模式下进行，具体操作步骤为：点击控制面板找到用户账户和家庭安全，选择添加或删除用户账户，选择希望更改的 Administrator 账户，点击创建密码后，即可填入设置的管理员密码了。

（2）清理浏览器浏览痕迹

当我们在浏览网站的时候，该网站的 Web 服务器就会在我们的计算机上新建一个 Cookie，Cookie 会将我们在网页上所输入的文字或是一些

选择都记录下来，那么当下次我们再登录这个网站，该网站的 Web 服务器会先看看有没有它上次留下的 Cookie 资料，有的话就会依据 Cookie 里的内容来判断使用者的身份、喜好。Cookie 的设置本来是为了方便我们浏览网站，但却被黑客利用，如果你没有清理浏览器为你储存下的 Cookie 资料，他们就有可能通过病毒或者木马获取你的电脑中储存的 Cookie，这就相当于他们获取了你在这个网站的身份，因此清理浏览痕迹对保护我们的个人隐私信息保护十分重要（图 5-2）。

图 5-2　清除网页浏览痕迹

以谷歌浏览器为例（其他浏览器也都类似），清理浏览器浏览痕迹的步骤如下：

打开浏览器进入设置页面后，点击历史记录按钮，看到清除浏览数据的选项，如（图 5-2），选择 Cookie 数据、浏览记录和缓存的图片和文件后，点击清除数据即可。

此外，当在网站上有登录操作时，不要点击叉号关闭浏览器，要先点击网站上“登出”“退出”或“注销登录”等按钮后退出自己的账户，再关闭浏览器，防止黑客盗用你的网站账户身份，进行违法操作。

（3）安装杀毒软件

各种病毒的流行给全世界的计算机系统都造成很大威胁，特别是2017年的Wannacry勒索病毒，病毒爆发后，不管个人用户、学校、银行或企业，“打开电脑”都成了最危险的操作，一旦感染这种病毒，电脑自动锁定，只有向黑客指定的账户打钱才可能解锁电脑。因此，安装杀毒软件的重要性凸显。大多数杀毒软件都有实时监控程序，还可以提醒你定期扫描杀毒并及时更新系统漏洞补丁。

现在市面上的免费杀毒软件种类很多，性能大都相差无几，可以选择自己喜欢的杀毒软件进行安装。

（4）废弃硬盘要进行特殊处理

信息技术发展迅速，电脑的更新换代速度也随之提升，在更换电脑时，会面临电脑的废弃硬盘处理问题。大多数用户在废弃电脑之后对硬盘的处理十分随便，以为只要将电脑硬盘内的数据格式化就可以了，但其实经过格式化后的数据只是在电脑内被搬了家，这些数据还原封不动地保留在硬盘内，黑客甚至对信息技术略懂的人都可轻易地恢复格式化后的硬盘中的数据，获取你的隐私信息。

个人和单位在处理废旧电脑时，如果硬盘中含有你不想被人知道的隐私信息，最好考虑用物理的方法销毁电脑硬盘，比如将硬盘内的盘片打孔或毁坏，以防硬盘内数据被盗取。

（5）使用“文件粉碎”功能删除文件

与废弃硬盘的原理相同，单纯删除文件并不能真的使这个文件在电脑中消失。因此在删除重要文件时，不要使用系统自带的删除功能一删了之，而应当使用杀毒软件自带的“文件粉碎”功能，对文件进行彻底的不可恢复性粉碎。

4. 个人移动设备安全防护

十几年前，我们的手机还没有现在这么多的功能，主要就是用来打电话或者发短信，近些年移动互联网飞速发展，智能手机和平板电脑迅速普及，我们使用移动设备的习惯发生了巨大的变化。现在，我们生活中的每个方面都需要使用到移动设备，从娱乐社交再到购物，收发电子邮件，查看天气地图，手机中储存着我们的各类信息，其包含的信息价值也越来越巨大。一台没有密码的手机被不法分子捡到后可以让手机主人遭受巨大的财产损失和信息泄露，那么我们应该如何保护自己手机上的信息呢?

（1）设置锁屏密码和应用锁

手机上的应用众多，有些应用，比如游戏、音乐 App，被不法分子打开对用户没什么影响，但有些应用十分重要，一旦被打开就会造成用户的财产损失，比如支付宝、微信、QQ 这类含有支付功能的软件，为了防止手机丢失时可能造成的信息泄露和财产损失，设置锁屏密码和应用锁十分重要。

大多数手机设置锁屏密码的方法类似，其步骤如下：一般手机中点击设置中的安全选项，找到屏幕锁定（有时也称屏幕安全保护等）后就可以选择设置图案密码或数字密码。

一般在手机安全管理软件中有设置应用锁，可以选择喜欢的软件下载之后，设置应用锁，一般来说，应用锁最好与锁屏密码不同。

（2）选择可靠的公共 Wi-Fi 连接

为了节省自己的运营商流量，许多人会在公共场所选择连接免费 Wi-Fi 联网使用手机，但现在的各种公共 Wi-Fi 种类复杂，如果手机连接的 Wi-Fi 并不安全，黑客就可以盗取你使用手机时传输的信息，如果你在连接 Wi-Fi 时进行了登录、支付操作或者传输照片，则黑客就可能得知你的密码，获取你的私人照片信息。

因此在连接公共场合的免费 Wi-Fi 时，需要谨慎，最好选取可靠的官方的免费公共 Wi-Fi，比如火车站、机场的 Wi-Fi，或先通过手机管家进行网络安全检测后再使用。此外，在公共场合使用免费 Wi-Fi 时，尽量不要网购或登录网银、第三方支付平台，防止用户个人信息、重要账号、密码泄露。

（3）谨慎点击链接或扫描二维码

在信息技术在各行各业广泛运用的今天，诈骗技术也随之升级。不法分子经常通过发送“你好，我在 × × 网站看到你，对你很感兴趣，我的照片点击下面的链接（或者扫描下面的二维码加我）”这类的短信，在其中放入下载木马的链接或二维码，从而操控受害者的手机，实施转账等犯罪行为。

因此，在日常生活中不要随意扫取识别陌生的二维码，当你无法判断短信或电话是否是真实地址发过来的时候，可先咨询客服，不要急于点击短信里的网址，以免被骗。

（4）关掉不需要使用的功能

现在我们的手机功能越来越多，比如位置、蓝牙、投屏、Wi-Fi 等，但这些本来是为了方便我们的功能，如果我们不小心使用，就有可能反而成了不法分子获取个人隐私信息的快速渠道。比如如果我们一直开着位置功能，各类 App 就将一直采集我们的位置信息，别人就可能通过一定的方式定位到你。而如果一直开着 Wi-Fi，可能我们会在不经意间连接上不可靠的公共 Wi-Fi，被盗取个人信息。

因此，在使用手机时注意将不需要的功能关闭，仅在需要的时候打开。

（5）不要卖掉废弃手机

在处理报废的手机时尽量不要选择卖掉或者扔掉，最好是在清空信息后统一放在一个地方搁置，因为即使手机恢复出厂设置，之前在你手机上储存的信息也不会彻底消失，技术人员通过一定的方式就能复原出你删除的内容，泄露你不想让别人知道的信息。

除了手机以外，废旧电脑、移动硬盘、U 盘等都不要卖给二手商家。如果想要彻底清除信息，需要先格式化数据存储后再覆盖无关数据，如此反复多次才能避免隐私信息被恢复。然而这对大多数人而言还是有一定难度的，也比较麻烦，因此也可以考虑进行物理销毁以保证绝对安全。

第二节　科技保护隐私

1. 科学界为隐私保护努力

各行各业的人们都从大数据的飞速发展中看到了价值和潜力，大数据开始与众多领域有所联系。然而随着大数据技术的广泛应用，出现的安全问题也越来越多。因此，广大科研人员在考虑通过隐私保护技术，寻求一些使用数据的方法，既不妨碍第三方从带有敏感信息的数据集中获取信息，挖掘大数据的价值，同时又避免隐私资料的泄露，为人们生活带来便利。

2016（首届）中国隐私保护学术会议邀请了国内外著名专家学者就大数据时代下的隐私挑战、隐私保护模型和隐私保护技术进行了探讨，探讨大数据隐私安全技术所面临的关键性问题和研究方向，推进我国隐私保护技术的研究与应用达到国际领先水平，切实保护公众的隐私安全。

在大数据应用背景下，中国人民大学的孟小峰教授对大数据隐私保护问题进行重新定位与思考，并试图从数据管理的角度探讨主动隐私管理技术，为大数据隐私技术提供新思路和理论依据。他认为与传统隐私泄露问题的本质有所不同，大数据时代的隐私问题是数据融合、数据分析、数据过度收集等造成的，所以我们要将隐私重新分类定位，变被动保护为主动保护，隐私风险监测与评估、主动保护、问责技术并行。风险监测与评

估达到事前预警的目的，主动保护提供事中整体防御措施，问责技术提供事后溯源和追踪，三者三位一体，形成一个完整的主动防御体系。此外，他还认为，隐私问题永远是一个开放的问题，人们一方面要开放共享，互联互通，另一方面又要隐私权，如何在这其中找到一个平衡点还需拭目以待。

中国信息通信研究院技术与标准研究所的何宝宏所长指出，数据流通是大数据产业的重要环节，但中国规范的数据交易缺乏有效管理机制，因此“是否需要对所有信息设定相同的隐私保护边界？”成为长期困扰着数据流通行业从业人员和监管人员的问题。在数据交易过程中，何宝宏所长强调了匿名化过程不能还原，并且要在收集数据时对用户关心的问题做出真实承诺，交易中有第三方评估监督和信息公开，交易后有规范的风险损失赔偿机制。但数据流通行业没有合规性标准和审计监督制度，因此，要实现这个目标，目前亟待统一规范数据的应用范围、授权的要求和流程、能够交易的数据类型和要求、交易方法、定价指导等。

复旦大学的周水庚教授指出查询处理隐私保护是大数据隐私保护的核心。大数据的价值是通过使用来实现的，使用数据也就是访问数据。在查询处理隐私保护中，根据角色将数据相关者划分为数据拥有者、数据使用者和数据服务提供者。不同角色对隐私的需求不同，数据拥有者需要数据隐私和存储隐私，数据使用者需要查询隐私，数据服务提供商需要数据隐私和查询隐私。隐私保护是大数据应用的关键，而查询处理的隐私保护是大数据隐私保护的重要环节。我们应结合现有数据管理技术、密码与信息安全技术，在实现高效安全算法、复杂查询处理的同时，保护数据、查询和存储隐私。

为了推进大数据时代个人隐私保护，2018 年 10 月，“第七届亚太地区隐私保护学者联盟国际会议”在南京邮电大学召开，国内外数十位专家学者与会。专家聚焦大数据时代的法律问题，系统梳理数据和隐私保护领域的最新进展、趋势和挑战，共同探讨新技术发展过程中出现的数据和隐

私保护等热点问题。

“在人工智能与大数据时代，数据的挖掘、整合、交易越来越便利，各种数据使用主体对个人信息的掌握越来越深入。大量个人信息在网络上存储、生成、被使用和交换，这一方面方便了人民的生活，另一方面也增加了侵犯个人隐私行为发生的可能性。”南京邮电大学副校长张志华表示，隐私数据保护渐成全球性问题，许多国家在争相制定实施符合自身社会发展与公众利益的数据保护政策及法律法规。中国一贯重视数据及个人信息保护，已颁布数十部法律法规保护公民的隐私，维护个人信息安全。他建议，要从技术与立法两个方面同时推进数据保护工作。一方面，在技术上保证数据来源与处理方式的透明性以及载体的安全性。另一方面，在立法上明确相关法律规定，通过完善相关立法，依法严厉打击非法泄露和出售个人数据等行为，推动形成统一有序的法律环境。

除此之外，国家对于大数据安全和隐私保护也大力支持。2018 年 5 月，贵州省大数据领域技术榜单“大数据安全与隐私保护关键技术”项目启动，对公共大数据安全、隐私保护等课题开展研究。“大数据安全与隐私保护关键技术”项目启动后，主要围绕公共大数据安全基础理论与方法、公共大数据隐私泄露风险评估与隐私保护技术、公共大数据安全技术应用示范三个课题进行研究。

贵州省大数据领域技术榜单中的公共大数据安全与隐私保护方向，主要针对大数据在开放、共享、交易和应用过程中的数据安全、隐私保护、数据滥用监管、风险评估等紧迫安全需求，组织开展大数据开放共享环境下的新型数据安全保护理论和算法研究，基于“云上贵州”应用平台推进相关标准和规范的制定。

2. 大数据隐私保护技术

目前研究人员在大数据的发布、储存、挖掘和使用阶段研究出了一定的技术成果，用来保护大数据交易过程中用户的隐私安全问题。

（1）大数据发布阶段

大数据听起来离我们很远，但其实它正是由我们日常生活中的各种活动组成。一般大数据的发布者包括政府部门、数据公司、网站或者用户本身等。与传统的数据发布相比，大数据的发布过程需要面临的风险更大。其中一个重要的原因是因为大数据的发布是动态的，与一个用户有关的数据就总量巨大、来源众多。因此，在数据发布时，发布者一定要对数据进行匿名处理，以保护用户隐私不被泄露。目前有大数据静态匿名技术和大数据动态匿名技术等。

在大数据静态匿名技术中（图 5-3），发布数据的机构需要对数据中准标识码进行处理，使得能有多条记录都具有相同的标识码组合。这样数据就不再具有独特性，黑客在进行链接攻击时，对于每一条记录的攻击都能同时关联到其他的许多条记录，从而使得黑客无法确定哪条是与特定用户相关的记录，从而保护用户隐私。

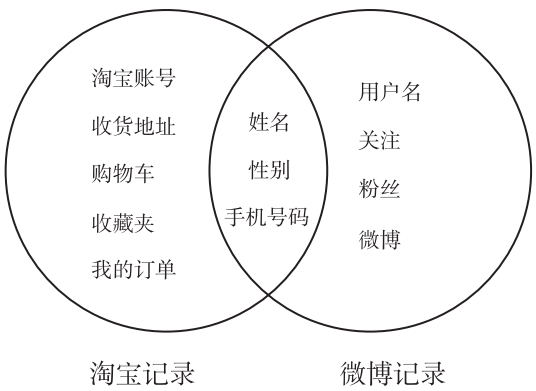

图 5-3　数据静态匿名处理

在大数据的动态匿名技术中（图 5-4），研究人员通过在原始的用户记录中引入一部分的虚假用户记录来保证黑客无法通过推理找到与特定用户有关的隐私记录。这些引入的虚假用户记录不对应任何原始数据记录，研究人员还在这些记录中引入了额外的标识符，混淆黑客的推理。

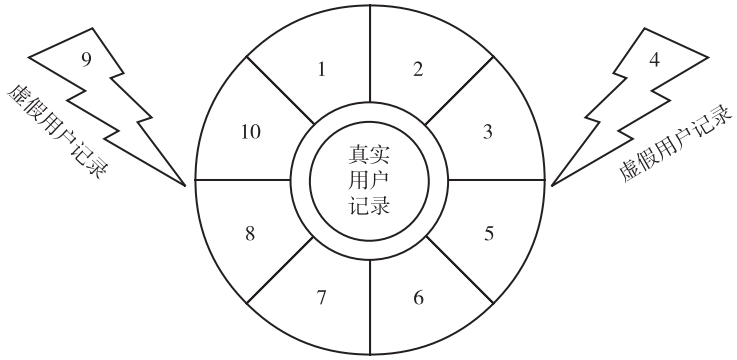

图 5-4　数据动态匿名处理

（2）大数据储存阶段

由于云的存储能力强，对大数据的访问也更快速和便宜，数据拥有者一般使用云存储平台储存大量的数据。但目前大部分云存储平台都不是发布数据的机构，即大数据的存储者和拥有者是分离的，因此云存储平台并不能保证是完全可信的，用户的数据面临着被不可信的第三方偷窃数据或者篡改数据的风险。与传统的数据存储阶段不同，大数据的查询、统计、分析和计算等操作也需要在云端进行，因此确保云端的大数据安全可靠十分重要。目前主要的研究结果有大数据加密存储技术。

大数据加密存储技术是在传统加密算法的基础上，将对称、非对称等加密技术进行了综合应用和完善之后研究出的适用于大数据时代的加密能力更强的方法。传统对称加密技术是发信方通过一定方法将文件加密后传输，收信方使用密钥和相同的方法解密文件（图 5-5）。

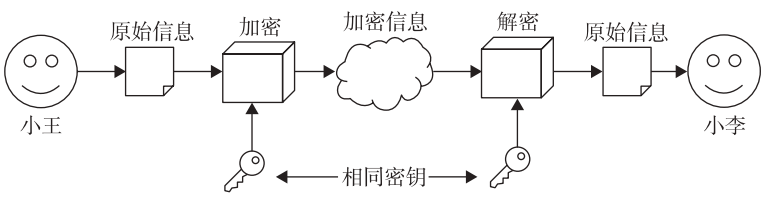

图 5-5　对称密钥原理

传统非对称加密技术中，发信方和收信方都分别有自己的公开的用于加解密的公钥和别人所不知道的私钥，发信方先使用收信方的公钥加密文件后传输，收信方可以使用只有自己知道的自己的私钥解密文件（图5-6）。

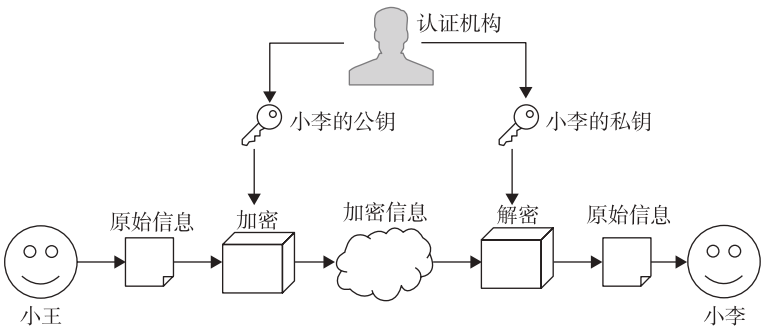

图5-6 非对称密钥原理

大数据加密存储技术中，一般先通过非对称加密技术加密文件内容，然后将这些加密后的文件储存在不同的各处，然后又使用对称加密技术对文件的加密密钥再进行加密，并将加密后的结果储存在数据中。这样经过多层次的多次加密，可以有效保证大数据的安全。

（3）大数据挖掘阶段

数据挖掘是大数据得到如此多的关注的主要原因。数据挖掘是从发布的数据中尽可能多地分析挖掘出各种有价值的信息，在纷繁的数据中找到关联性。大数据环境下的数据在发布时一般都经过匿名等处理，但在数据挖掘技术如此发达的今天，经过大数据关联分析、聚类、分类等数据挖掘处理后，依然可以从处理过的大数据中分析出用户的隐私。目前主要的隐私保护技术有关联规则的隐私保护和分类结果的隐私保护。

关联规则可以从一个方面解释事物之间的某种联系，支持度一般表示两种事物同时出现的频率，置信度表示一种事物出现时，另一种事物出现的可能性（图5-7）。关联规则的隐私保护主要是通过一定的算法修改支

持敏感规则的支持度和置信度，使它们小于一定的值，从而降低两种事物同时出现的频率，也就降低了数据之间的关联性，这样一来，黑客就不那么容易找到与特定用户有关系的各种隐私信息了。

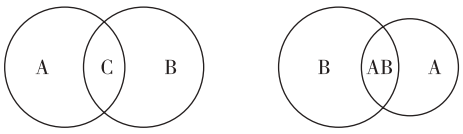

图 5-7　关联规则的隐私保护

分类结果的隐私保护是通过一定的算法对数据进行分类处理，发现数据中的隐私敏感信息，从而专门对分类出敏感数据进行特殊保护（图 5-8）。这种方法不仅可以降低敏感信息被黑客发现的可能性，还不会影响其他应用的功能。

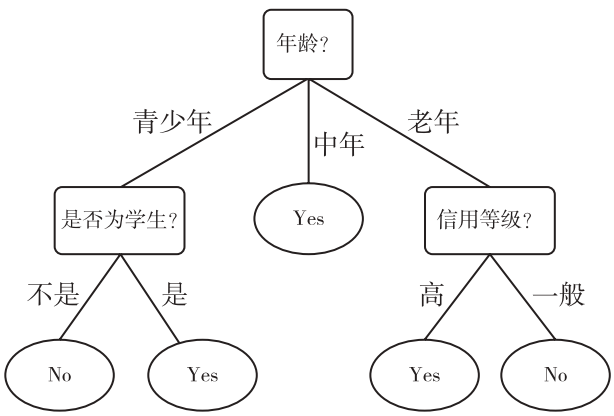

图 5-8　分类结果的隐私保护

（4）大数据使用阶段

目前大数据的大部分使用者都是企业。企业通过使用大数据，可以分析潜在用户的范围，迎合用户的喜好销售自身商品，或者提高用户的使用体验，为企业创造更大的价值。如何确保合适的数据在合适的时间和地

点，给合适的用户访问和利用，是大数据使用阶段面临的最大风险。为了更合理地限制大数据的使用，研究人员提出了访问控制技术。

访问控制技术主要用于决定可以访问的用户群体，用户访问的权限等问题，通过限制访问的范围在一定程度上解决大数据使用过程中的隐私保护问题。目前，各类社交网站允许用户在转发或发布信息时，通过分组决定哪些信息可以被哪些人看到，这就是一种访问控制。与传统的访问控制技术不同，现今一个用户有时可能需要访问不同种类的数据，因此大数据下的访问控制技术需要为每个用户分配每个场景下合理的使用权限、鉴别异常用户、动态更新用户的权限和角色（图 5-9）。

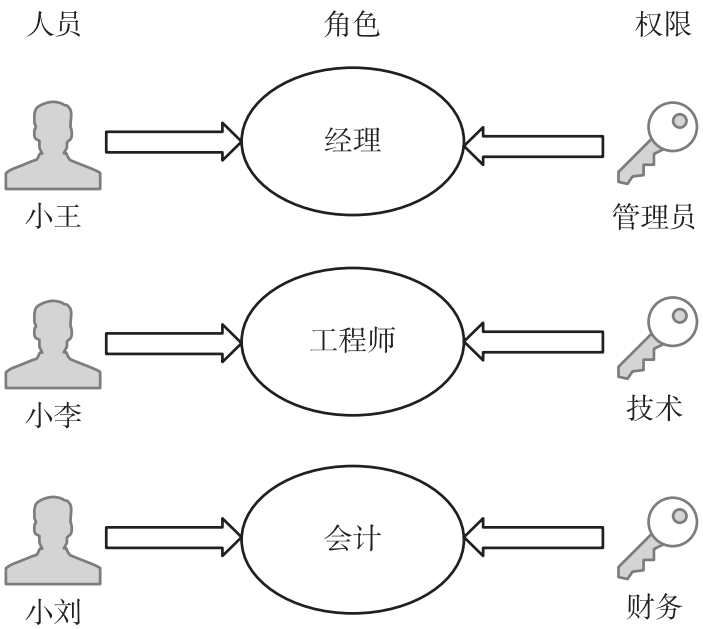

图 5-9　访问控制技术

第三节　行业社会保护

大数据技术的发展是以互联网行业为基础的，公众的个人信息在互联网上产生、储存、搜集、开发、利用、传递和营销，且互联网的数据使用范围广泛、表现形式多样、传播速度快，尤其是互联网的网络共享性与开放性使得人人都可以在互联网上获取和存放信息。

但是我国关于在互联网上保护隐私信息的法律和法规政策不完整，约束力较差。尽管许多的网站都有关于用户隐私保护的政策条款，但是这些条款都是一些基本的条款，没有具体的保护范围和对象，也没有关于违反这些隐私保护政策的处罚和责任；另外，这些政策都是网站自身设定的，并没有征求用户的意见，也没有相关的机构进行监督和认证，造成互联网行业自律性差，用户隐私存在安全隐患。

大数据技术的发展，加大了公众隐私信息泄露的可能性，也增加了隐私信息的管理难度。用户隐私的保护仅仅依靠国家法律政策、政府监督是远远不够的，还需要依靠网络行业的自律性才能实现。例如在网络行业中肯定存在有法律空白区域、政府监管不到的区域等，在这些区域中容易滋生矛盾、冲突，容易侵害用户的隐私等权利，这就需要互联网行业有很好的自律性，来自觉地弥补这些缺陷，承担起自己的社会责任，共同维护人民的合法权益。

此外，行业协会准则能确定一些具体的权利义务内容，从而达到数据保护法规定的确定性与透明性要求。比如网站的隐私政策或隐私声明不能采用模糊化处理，必须明确地说明哪些个人信息将会被收集、所收集的个

人信息将用于何种用途以及信息主体的权利条款等内容，违反上述规定的隐私政策或声明将受到行业协会的处罚或成为司法过程中的不利证据。行业协会准则不具备法律效应，更多的是从商业道德方面对服务商进行规范，实现行业自律，可以称为一种社会“软强制”，相比正式法律的“宣言式条款”具有更强的认同感和执行力。且在数据收集和利用过程中的个人信息隐私侵权情况发生时，行业协会的处理更灵活，成本也更低廉，是信息隐私侵权纠纷解决的最佳选择。

美国的行业自律模式在公民个人隐私保护问题上发挥着举足轻重的作用。首先，在整个互联网、电子商务、大数据行业内建立相应的行业自律组织，并由该组织确定本行业有关隐私保护的基本原则、具体的保护措施与实施规范，所有组织成员都必须承诺并遵照原则与规范开展经营活动。

其次，美国的互联网企业为了构建一个相对安全的信息传输环境，自发建立了多种网络隐私安全认证体系，对不同的机构、网站进行验证，向其中符合隐私保护要求的网络服务商颁发证书，广大用户便可通过观察证书的有无，判断自己选择的网络服务商是否能尽到个人隐私保护义务。

最后，电脑中装载的杀毒软件也会对各种自动搜集个人信息的情况进行警示，行业自律模式不仅增加了作为网络服务商的隐私保护义务，同时也要求用户对自己的个人隐私负责，再从客观条件上为隐私保护供助力，通常能收到较好的保护效果。

大数据时代下，我国法律对公民隐私保护力度有所匮乏，在这种情况下，行业社会的保护不失为一种有效的规制模式。即使制定了有关的法律，行业社会保护仍不会因此失去其存在的价值和意义，它会同相关的立法相结合，继续发挥其应有的作用。我国行业社会从以下几个方面来保护公民的隐私安全。

（1）行业协会准则

2012 年 11 月 1 日，中国互联网协会发布了《互联网搜索引擎服务自律公约》，其中第十条规定：“搜索引擎服务提供者有义务协助保护用户隐

私和个人信息安全，收到权利人符合法律规定的通知后，应及时删除、断开侵权内容链接”。值得一提的是，该公约第一次明文规定搜索引擎企业必须遵守国际行业惯例和规则，遵守机器人协议（Robots 协议），百度、奇虎 360、搜狗、腾讯、新浪等 12 家搜索引擎企业签署了该公约。

2017 年年底，全国信息安全标准化技术委员会归口的《信息安全技术：个人信息安全规范》正式发布，并作为国家推荐标准将于 2018 年 5 月 1 日正式实施。其中明确了权责一致、选择同意、最少够用等关键性技术原则。

（2）企业政策

除了行业发布的自律公约外，一些网站的经营者及网络服务商也制定了网络隐私保护声明。2017 年 7 月，中央网信办、工信部、公安部、国家标准委对包括腾讯、京东和百度在内的 10 款网络产品和服务的隐私条款评审，规范其收集、保存、使用、转让用户个人信息的行为，督促整改不合法的条款，百度、京东等大型互联网企业调整隐私政策，在对个人信息的使用上均作出相关规范。

京东在整改生效的版本中，明确了京东的产品与 / 或服务收集、使用及共享个人信息的类型方式和用途；以增强告知或即时提示的方式在收集、使用及共享个人信息时给予用户明示选择权，并在产品设置中允许用户即时撤销授权。同时明确了用户查询、更正和删除其个人信息的方式，且增加了用户账户的锁定 / 解锁和注销功能，并提供给用户了 30 日注销后悔期。在一个月的“后悔期”内，用户可以随时申请恢复已注销的账号。

百度地图提及会以“最小化”原则收集、使用、存储和传输用户信息，在其网络隐私保护声明中规定，只有在用户自愿选择服务或提供信息的情况下才会收集用户的个人信息。用户使用百度的服务时，会被告知相关信息的使用目的和范围，比如服务器会自动记录哪些信息、网站在什么情况下披露用户的个人信息等。

（3）社会部门

为摸底我国相关信息网络安全情况，我国于 2018 年开展为期半年的全国网络安全执法大检查，大数据安全整治是行动中的重要内容，具体包括大数据的采集、存储、应用、传输、销毁等全生命周期的监管、安全以及保护。

这次行动首次将大数据安全纳入检查对象，更是将针对公民个人信息的保护放在执法的重要位置。大数据安全整治将全面对我国大数据信息内容、存储位置、所涉企业进行摸底。同时，对企业采集信息来源开展执法检查，对数据采集的合法性、应用的范围限制等进行确定，对合法采集内容与非法采集内容进行分类。对于非法采集信息，将进行集中打击、销毁，对合法、合规采集的信息，则纳入保护监管范围。

第四节 国家法律与政策保护

互联网的发展使得人与人之间的关系更紧密，但也使得很多企业、机构可以搜集并储存人们的个人信息，比如电商网站、快递公司、房地产中介等，他们需要组织用户信息形成庞大的数据库以进行大数据分析和计算。但有时由于网站存在安全漏洞，或者内部管理制度的不严谨，一些员工或黑客受利益引诱，铤而走险，通过自身权限，或通过攻击网站漏洞获取并倒卖用户的个人隐私信息，由此催生出的电信诈骗等犯罪不仅造成用户财产损失，公司的名誉也会因此受到影响。

因此，为了更好地规范企业使用用户大数据，同时也防止个人倒卖隐私信息的现象再盛行，国家建立了相关的行业规范制度和法律法规，对个

人和企业都进行约束。不过由于目前大数据技术还在动态发展中，针对大数据时代下的隐私保护的相关法律法规还在不断摸索和完善，要真正实现用户隐私保护还有很长一段路要走（图 5-10）。

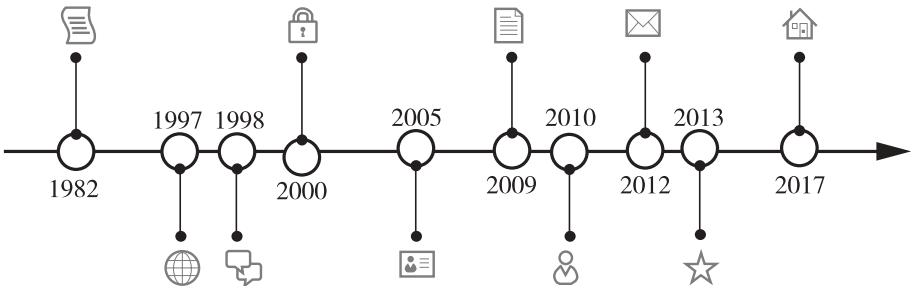

图 5-10　隐私保护发展史

在 1982 年的《中华人民共和国宪法》中，我国就规定了有关人权、身体权、人格权、住宅权，通信自由与秘密的条款，以此来保护公民隐私。随着信息时代来临，隐私的含义开始变得丰富，过去的司法解释已不足以保护新时代下的个人隐私。

1997 年，公安部发布了《计算机信息网络国际联网安全保护管理办法》，通过保护互联网中的通信自由与通信秘密来保护公民的个人隐私。在第七条中明确指出“用户的通信自由和通信秘密受法律保护。任何单位和个人不得违反法律规定，利用国际联网侵犯用户的通信自由和通信秘密”。

1998 年，国务院颁布了《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》。该办法直接对侵犯个人隐私的行为进行约束，在第十八条中明确“用户应当服从接入单位的管理，遵守用户守则；不得擅自进入未经许可的计算机系统，篡改他人信息；不得在网络上散发恶意信息，冒用他人名义发出信息，侵犯他人隐私；不得制造、传播计算机病毒及从事其他侵犯网络和他人合法权益的活动”。以此严禁互联网用户在网络上散发恶意信息，冒用他人名义发出信息，侵害他人隐私。

2000 年，全国人大常委会第 19 次会议通过了《关于维护互联网安全的决定》，将利用、侵害个人隐私的行为上升到了犯罪的高度，决定对“利用互联网侮辱他人或者捏造事实诽谤他人、非法截获、篡改、删除他人电子邮件或者其他数据资料，侵犯公民通信自由和密码通信，以及利用互联网进行盗窃、诈骗、敲诈勒索”的行为，依法追究刑事责任。

2005 年，新修订的《妇女权益保障法》中，隐私权被作为与名誉权、荣誉权、肖像权相对等的人格权受到法律的保护。

2009 年,《刑法修正案七》进一步对非法获取、出售、非法提供公民个人信息犯罪做出了规范。

2010 年开始执行的《侵权责任法》中，隐私权进一步被确定为我国公民的民事权益之一，其中第三十六条针对新时期网络侵权频发的现状，对网络侵权的救济与责任承担做出了较为细致的规定，为我国公民保护网络活动中的个人隐私保护提供依据。

2012 年，全国人大常委会在《关于加强网络信息保护的决定》中进一步加强了对个人的隐私保护，其中第一条就明确将“能够识别公民个人身份和涉及公民个人隐私的电子信息”纳入保护范围，并在随后的三条中，对我国公民网络隐私保护的义务主体进行明示，对各主体的行为规范进行了详细的阐述。第七条还对近些年日益猖狂的垃圾邮件、垃圾短信问题进行了规范。第八条、第九条和第十条对公民隐私信息泄露后，公民的权利和有关组织及机构应该承担的义务进行了规定。

2013 年，工信部推出《信息安全技术公共及商用服务信息系统个人信息保护指南》(下文简称《指南》)，在指南中，不仅对个人信息主体、个人信息管理者和个人信息获得者进行了明确说明，还突破性地对个人信息的类别进行了划分，对个人敏感信息和个人信息进行区分，规定个人信息为“信息系统所处理、与特定自然人相关、能够单独或通过与其他信息结合识别该特定自然人的计算机数据。个人信息可以分为个人敏感信息和个人一般信息两种”。明确个人敏感信息为“一旦遭到泄露或修改，会对

标识的个人信息主体造成不良影响的个人信息。各行业个人敏感信息的具体内容根据接受服务的个人信息主体意愿和各自业务特点确定。例如个人敏感信息可以包括身份证号码、手机号码、种族、政治观点、宗教信仰、基因、指纹等”。对于个人信息与个人敏感信息，根据其差异有差别地进行隐私保护。

《指南》借鉴了国外的先进经验，参照国外现有的保护模式，确立了我国利用、处理个人信息的八项原则：个人同意、目的明确、公开告知、最少够用、诚信履行、质量保障、安全保证、责任明确。具体条款如下：

（1）目的明确原则——处理个人信息具有特定、明确、合理的目的，不扩大使用范围，不在个人信息主体不知情的情况下改变处理个人信息的目的。

（2）最少够用原则——只处理与处理目的有关的最少信息，达到处理目的后，在最短时间内删除个人信息。

（3）公开告知原则——对个人信息主体要尽到告知、说明和警示的义务。以明确、易懂和适宜的方式如实向个人信息主体告知处理个人信息的目的、个人信息的收集和使用范围、个人信息保护措施等信息。

（4）个人同意原则——处理个人信息前要征得个人信息主体的同意。

（5）质量保证原则——保证处理过程中的个人信息保密、完整、可用，并处于最新状态。

（6）安全保障原则——采取适当的、与个人信息遭受损害的可能性和严重性相适应的管理措施和技术手段，保护个人信息安全，防止未经个人信息管理者授权的检索、披露及丢失、泄露、损毁和篡改个人信息。

（7）诚信履行原则——按照收集时的承诺，或基于法定事由处理个人信息，在达到既定目的后不再继续处理个人信息。

（8）责任明确原则——明确个人信息处理过程中的责任，采取相应的措施落实相关责任，并对个人信息处理过程进行记录以便于追溯。

《指南》虽然仍属于行业指导性规范，不具有法律效力，但是由于其

前瞻性与先进性，对我国完善个人信息的隐私保护有着极为重要的意义，对完善大数据隐私保护立法也有着极为重要的参考价值。

2017 年 6 月 1 日,《中华人民共和国网络安全法》正式实施，这是对我国公民个人信息保护一次有力的加强。该法强调，个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。并对个人敏感信息的处理做出了单独说明。

《网络安全法》中规定，任何互联网企业在收集和使用公民信息时，必须遵守“合法、正当、必要”的原则，网络运营者不得收集与其提供的服务无关的公民个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用公民的个人信息，并且网络运营者收集、使用公民的个人信息，应当公开其收集、使用规则。

此外,《网络安全法》第三十七条中还指出，公民发现网络运营者违反法律、行政法规的规定或者双方约定的收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储个人信息有错误的，有权要求网络运营者予以更正。

其次,《网络安全法》在严格规范网络运营者的数据保护责任方面，明确要求一旦发生泄露、毁损、丢失的情况，网站方必须及时采取有效措施降低危害，或采取技术等手段及时进行补救，并且按照规定及时告知用户并向有关主管部门报告。

大数据时代的到来，对政府管理产生了巨大影响，催生了政府数据开放。政府数据开放网站的个人隐私政策直接关系到开放过程中个人隐私是否得到充分保护，但是立法中并没有涉及政府信息系统安全。总的来说，我国不是没有网络安全法律法规，而是缺乏一个完善的法律制度体系，尤其是缺乏一部能统筹网络安全各种关系的基本法。

总的来说，我国大数据的个人隐私保护还处于起步阶段，但随着信息

技术的发展以及数据以几何级数的飞速增长，个人信息及隐私保护将受到巨大挑战。数据收集无处不在，数据用途不断被挖掘，个人信息和非个人信息越来越难以区分，面对这些挑战，法规中的以“告知与同意”为框架的条例越来越难以发挥作用。

第五节　国际隐私保护经验

国外隐私权法律保护制度相较于国内起步较早，有很多我们可以借鉴的经验，下面介绍美国和欧盟隐私保护的经验以供参考。

1. 欧盟

在欧盟，个人隐私信息保护的总体情况是重公法保护，轻私法保护，1995 年颁布的《个人数据保护指令》强调个人信息保护，追求信息自主、信息控制和信息自决。此后，为了应对大数据环境下的个人隐私保护新挑战，2016 年通过了新的数据保护法案 GPDR（General Data Protection Regulation，通用数据保护指令）并于 2018 年生效。

GDPR 是世界范围内最严格的用户数据保护条款，所有在欧盟境内经营或搜集和处理欧盟公民数据的外国企业都要遵守该法律。条例对数据收集者的操作规范和用户对自己数据完全自主的权利提出要求。

规定数据收集者不能用隐藏默认的方式获取用户许可，必须提前进行明确的提示与询问，获得允许后才可以获取使用用户数据；收集之后还需要为用户提供查看收集数据概览及用途，还必须有用户删除功能。

在用户权利方面，用户对自己的数据拥有完全的所有权，即便同意收集方收集，也可以随时查看撤回删除相关协议，在用户撤回删除相关授权

后，数据收集者必须立即将相关数据进行匿名化处理。

不论是早期的《个人数据保护指令》还是新颁布的 GDPR，均体现了欧盟国家在个人信息保护领域统一化、标准化和一体化的立法和执法特点。欧盟国家将个人信息等同于个人隐私，从个人信息的采集，到信息的使用和交流，一直到信息的销毁，整个信息的全流程、全周期都有很明确的行为规范要求。

在个人信息的采集环节，要求正当合法地获取和处理，实行“最少采集”原则，要尽量少地采集个人信息，采集之后只能用于特定目的，不能用于非采集的目的。相关机构采集到个人信息后，要建立一套安全保护制度，采集信息的目的达到后，要在一定期限之后予以销毁。同时，欧盟很多国家都建立了个人信息处理的许可或登记制度，经过许可才能进行信息收集。

在信息采集后的使用环节和销毁环节，欧盟实行了独立的个人信息保护执法机制，专设有信息专员，监督信息在使用过程中的权限和范围。如果个人隐私信息被非法使用或者贩卖，有相应的法律责任的追究和法律救济渠道，除了进行罚款，对违反法律泄露个人信息者还可以处以刑事责任。

作为个人信息的最大拥有者——政府机构，也同样和其他私有主体一样受到法律监管。欧盟设立的独立信息保护机构可对政府机关的个人信息泄露采取法律制裁。信息保护机构还可对企业的个人信息泄露行为进行检查、要求整改和定期报告，并追究法律责任。此外，该法律对于进入欧洲市场的企业也同样具有法律约束力，特别是向第三方进行个人信息转移，将受到法律的制裁。

2. 美国

相较于欧洲严苛的个人隐私立法保护机制，美国的隐私保护模式更灵活，使用行业自律与法律规范协同管理，自下而上地实现对民众个人隐私

权的保护。

当然，仅仅靠行业自律来保护个人隐私问题是不够的，还要靠法律与政府引导。除了行业自律模式，美国联邦政府下属部门就个人隐私保护问题，发布过多部指引性报告与架构设计，不仅将隐私权确立为“联邦宪法所保障的基本人权”，而且还拥有专门的《隐私权法》。除此之外，《健康信息与转移责任法》禁止卫生保健服务的供者不经患者同意而使用和泄露患者信息，其隐私保护标准在全球同业中被视为“金标准”；《GLB 法案》要求金融机构每年书面告知客户其隐私政策并向客户供选择主动退出的表格，使客户能够拒绝出售或分享其财务信息；《儿童在线隐私保护法案》则针对 13 岁以下的儿童的在线数据的隐私保护做出了专门的规定。这些法案均对因泄露个人信息造成的隐私问题做出了严格的规定，有效地保障了美国公民的个人隐私。

法律是保障居民权利最重要、最有效的手段，因此，要在立足我国基本国情的基础上来借鉴国外的立法经验，加快个人信息安全立法速度，具体和细化相关法律法规，规范企业对于数据使用和发布的管理，为监管部门提供有效的法律依据，形成一个具有中国特色的隐私权法律保护体系。

首先，需要把隐私权作为一项独立的人格权利进行保护，明确隐私权的界限、内涵，比如欧盟个人数据保护法指出，身份证号码、定位数据、网络标识符、生理、心理、基因、精神、经济、文化、社会身份等隐私受法律保护。其次，要加强对儿童、青少年、未成年人等一些特殊群体的保护，完善法律体系。最后，需要对于网络、政府等收集、利用居民信息的机构、单位、企业进行合理的规范约束，明确其权利和义务，规定其法律责任，加强对网络运营商的管理，经常进行网络信息的筛选、检查，禁止不利信息的发布。

第六节 隐私泄露后的补救措施

保护我们的个人隐私信息，最好的办法就是在日常做好安全防范措施，避免信息泄露。因此，我们从个人意识、科学技术、行业社会以及国家政策的角度讲述了如何防患于未然，保护公民的隐私信息不被泄露。

但是，百密一疏，再全面的防范措施也无法保证个人隐私信息的绝对安全，个人信息一旦被泄露出去，轻则被广告骚扰，重则被骗取钱财，甚至有人丧失生命。就目前来说，在日常生活中，如果自己的隐私信息被泄露，可以通过以下三种方式来维护自己的合法权益：

（1）按照全国人大常委会《关于加强网络信息保护的决定》，遭遇信息泄露的个人有权要求网络服务提供者立即删除有关信息或者采取其他必要措施予以制止。

（2）向公安部门、互联网管理部门、工商部门、消协、行业管理部门和相关机构进行投诉举报。国家网信办所属的中国互联网违法和不良信息举报中心将专职接受和处置社会公众对互联网违法和不良信息的举报。举报热线为“12377”，网址为 www.12377.cn。

（3）依据《侵权责任法》《消费者权益保护法》等，通过法律手段进一步维护自己的合法权益，如要求侵权人赔礼道歉、消除影响、恢复名誉、赔偿损失等。

那么这三种维权途径应该在哪种场合下使用呢？我们一起通过事例来了解一下。

林女士最近十分苦恼，她在网站上购物后频繁接到诈骗电话，不法分子知道订单上的所有信息，包括她的姓名、电话、邮寄地址和所购，甚至

下单时间和订单单号也都准确无误。而这个问题在我们日常的生活中也经常碰到，那我们遇到这种情况，应该如何维护我们的个人权益呢？

在《关于加强网络信息保护的决定》中第四条规定“网络服务提供者和其他企业事业单位应当采取技术措施和其他必要措施，确保信息安全，防止在业务活动中收集的公民个人电子信息泄露、毁损、丢失。在发生或者可能发生信息泄露、毁损、丢失的情况时，应当立即采取补救措施”。因此，遇到这种情况，我们可以向网购平台投诉，要求他们采取行动，对我们的订单信息进行处理，修改或者删除，避免我们的信息持续泄露。

同时，《消费者权益保护法》第五十条规定“经营者侵害消费者的人格尊严、侵犯消费者人身自由或者侵害消费者个人信息依法得到保护的权利的，应当停止侵害、恢复名誉、消除影响、赔礼道歉，并赔偿损失”。因此，如果此类事件严重损害了信息所有者的权益，我们可以请求法律保护，以此来维护自己的合法权益，向侵权人要求消除影响、赔偿损失。

对于更严重的个人信息泄露情况，我国法律也给出了保护方案。《中华人民共和国刑法》中对个人信息泄露给出了明文规定：“违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金”。

此外，针对一些网络服务提供者不履行网络安全管理义务，造成严重后果的情况，增加规定：“网络服务提供者不履行网络安全管理义务，经监管部门通知采取改正措施而拒绝执行，致使违法信息大量传播的，致使用户信息泄露，造成严重后果的，或者致使刑事犯罪证据灭失，严重妨害司法机关追究罪犯的，追究刑事责任”。

那么，因为泄露个人隐私事件而被处以刑罚的事件真的会存在吗？答案是肯定的。2013 年 4 月，李某伙同杜某等四人创立了一家有限公司，

他们的业务是电话推销假冒心血管保健品。后李某等人获悉，倪某手中有老年人的个人信息资料，于是将公司 10% 的股份分给倪某，并让其担任公司法定代表人。

李某等人之所以如此看重倪某，是因他们销售的假冒保健品有巨大利润，但必须知道老年人的信息。通过倪某的资源，大量老人上当，花了几万元，买来没有任何疗效的保健品。

公安机关在倪某的暂住地起获公民信息表 74 捆及电脑主机一台。经鉴定，倪某电脑中的公民个人信息达 125 万余条。经审理，北京丰台法院以非法获取公民个人信息罪，判处倪某有期徒刑 2 年，并处罚金 1 万元。

总的来说，我们在信息被泄露后可以采取以下措施，来减少或者消除损失：

（1）收集证据线索。在信息泄露之后，很容易收到各种各样的垃圾邮件，接到天南海北的骚扰电话。这时候要留心，记下对方的电话或者是邮箱地址等有用的信息。可能这些信息很琐碎，但是一旦收集好，不仅能帮助自己维权，而且还可能帮助更多的人。

（2）向相关部门报案。个人信息一旦泄露，可向公安部门、互联网管理部门、工商部门、消协、行业管理部门和相关机构进行投诉举报。报案的目的一来是保护自己的权益，二来也是备案。一旦有更多的人遇到和你类似的情况，就可以一起处理。根据刑法的相关规定，向他人出售或者提供公民个人信息以及非法获取公民个人信息情节严重的，可能涉嫌刑事犯罪，公安机关可以介入调查。

（3）提醒身边的亲朋好友防止被骗。个人信息泄露后，不仅可以用这些信息盗用你的账号，甚至还可能骗你身边的亲朋好友。所以一旦你的信息泄露，或者联系工具账号丢失，一定要第一时间通知你的亲朋好友，要他们倍加防范，以免上当受骗。

（4）委托律师维权。如果个人重要的信息丢失，而且知道怎么丢失的或者是有很多线索，那么就可以向专业的律师咨询相关的法律法规。

如果律师给予肯定的答复，就可以利用法律的武器维护自己的权益。如果是在消费过程中泄露，还可依据《侵权责任法》《消费者权益保护法》等，通过法律手段要求侵权人赔礼道歉、消除影响、恢复名誉、赔偿损失等。


第六章

未来如何保护隐私？

大数据时代，个人信息的非法收集和利用以及无处不在的数据监控给公民的信息隐私保护带来巨大威胁，传统的隐私保护方法已经全面陷入困境，无法应对新的挑战。在传统的规制手段中，“知情同意”有效性不足，匿名化、模糊化技术遭遇瓶颈，个人信息边界模糊，多元信息收集者尤其是第三方信息中介力量异军突起，在传统制度中难以寻求有效的适用规定，造成侵权责任界定不清与监管空白。

此外，信息主体对个人信息的主动披露、信息的不当泄露与机构、企业对信息无限度地挖掘，在不断制造并增加着侵犯个人隐私权的途径，带来隐私被曝光后心理的恐慌和生活中的伤害。我们向互联网企业提交个人信息换取便利，我们把数据信息储存在云端，我们将个人的点滴生活在社交网络上分享。个人信息的收集方式、使用目的及后果影响日趋失控，个人信息保护被前所未有地置于洪荒之地，面临严峻威胁。

然而，大数据的发展和应用是人类技术与产业进步的希望所在。只要数据被合理应用，大数据在医疗工程、民生工程和销售领域都可以发挥出巨大的能量，帮助我们获得更好的生活服务，提高生活质量，比如利用用户购物的浏览痕迹，分析用户的购物喜好，从而推送广告，带给用户更好的购物体验。因存在个人隐私泄露的风险而放弃大数据技术在现实生活中的应用，禁止对网络数据的分析和利用，这无疑是因噎废食。

在未来，保护隐私数据首先要转变的是个人观念，变被动为主动，这是大数据时代下个人隐私保护不可或缺的一环，同时也是最为重要的一环。我们要加强个人隐私的安全意识，在意识层面将隐私信息的保护放到一个重要的位置，认识到个人隐私保护的重要性，提升个人隐私保护意识，从源头上来保护个人的隐私数据。

个人提高隐私保护意识可以在一定程度上减少隐私数据的泄露，但大

数据技术要发展，就必然会有数据的应用，在数据应用的过程中，还要依靠技术手段来保证数据安全高效的应用。人工智能和网络态势感知技术的出现和应用，给大数据隐私保护技术带来了新的机遇，极大地提高了隐私数据的安全性。

第一节　人工智能打击黑产

随着大数据技术的高速发展以及数据价值的持续增长，隐私数据安全形势持续严峻，且呈现出智能化、隐匿性、规模化的特点，这让网络空间数据安全的防御、检测和响应面临更大的挑战。

黑产是黑色产业链的简称，是盗取他人信息和财产账号用于非法盈利的犯罪产业。不法分子利用运营商漏洞，在网页中植入恶意代码，在用户访问这个页面之后，窃取登录信息、手机号码等隐私数据，然后利用这些数据实施精准诈骗或贩卖信息等非法活动。隐私窃取黑产往往由三个层级组成，一级网站负责研发制作，二级网站负责销售，三级网站窃取信息，俨然已经发展成一个有组织、分层级的严密结构，给公民的隐私安全造成严重的威胁。

人工智能的出现给大数据时代的隐私保护带来了新的机遇。提到人工智能，人们最先想到的是机器人，但这仅仅只是人工智能的一个分支。人工智能是一个很宽泛的概念，从人脸识别到机器翻译，从手机上的智能软件到可穿戴设备，从无人驾驶汽车到未来可能改变世界的其他重大变革，但这些都有一个共同特点，它们仿佛拥有人的思想，可以进行思考。

简单来说，人工智能是研究使计算机来模拟人的某些思维过程和智能行为（如学习、推理、思考、规划等）的学科，主要包括计算机实现智

能的原理、制造类似于人脑智能的计算机，使计算机能实现更高层次的应用。从思维观点看，人工智能不仅限于逻辑思维，要考虑形象思维、灵感思维，尤其是基于大数据技术的人工智能，更是呈现出深度学习、跨界融合、人机协同、群智开放和自主智能的新特点。

目前，人工智能以其独特的优势，正在各类安全场景中形成多种多样的解决方案。利用人工智能，依托大数据、情报威胁、深度学习等技术来打击隐私窃取黑产就是其中之一。使用基于网页内容的算法和基于关系图的算法这两个维度的算法，对网页进行高效的安全检测，发现网页中存在的安全隐患和黑产网页之间的关联性。

在利用人工智能打击黑产时，首先使用独特的检测系统发现和检测网络黑产，对网页以及它们之间的关系进行广泛收集，然后把这些收集好的数据进行分类，基于这些有限的数据，通过一定的目标定义“教”机器去学习，去自动地智能识别黑产网页，当检测到这些不安全的网页的时候，机器就会智能地给这些网页打上风险提示标，提醒用户注意当前操作。

人工智能中的深度学习具有多层表征和抽象能力，能够自动发现很多黑产网页隐含的相关性，因为黑产会比较频繁地使用一个模板夹杂着不同的推广信息，当有很多这种黑产模板出现的时候，这些信息的相关性就很容易被黑产打击系统捕捉到，通过强大的数据监测平台，建立起网站的关系图谱，然后再结合数据挖掘的方法，就能从看似杂乱无章的关系中寻找到黑产的脉络，从而追踪到多个隐私泄露的源头，保护公民的隐私数据。

此外，在诈骗信息打击方面，可以通过大数据分析和机器自我学习、总结、预测警情中作案手法、通信行为、网络特征、资金流向等特点规律，从而能在诈骗事前、事中、事后等环节起到预警、分析作用。

人工智能系统还有一个很大的优势就是它能够快速识别上亿的网页，并且准确率非常高，相较于人工一天识别几千个页面的极限，可以 24 小时不断地识别下去，极大地提升了打击黑产的效率。

把 AI 的能力落实到网络安全治理上，可以提升安全治理的效率和

网络安全的防护能力。未来，随着人工智能技术日趋成熟，人工智能在“AI+ 安全”领域不仅能够全面提高对网络空间各类威胁的响应和应对速度，而且能够全面提高风险防范的预见性和准确性，进一步提升打击黑产的效果。

第二节　网络态势感知

信息和互连带来的不仅仅是便利和高效，大量隐私、敏感和高价值的信息数据和资产，必然引起不法分子等恶意攻击者的觊觎，隐私数据获取、渗透服务都是明码标价，攻击者已经不是曾经的兴趣驱动展示技术实力和自我价值，而是发展成为利益驱动、有组织的产业链，这带来的直接后果就是攻击者会采取更隐蔽的手段、更善于潜伏起来收集和窃取信息，给用户的隐私数据带来更大的安全威胁。

“智者千虑，必有一失”，即使是技术最好、最严谨的攻击者，在入侵系统窃取数据后也难免会留下可供防御者研究和分析的痕迹。实际上，通过分析国内外知名的隐私数据泄露事件，安全专家发现事后总是能够找到攻击者渗透和窃密的蛛丝马迹。因为一次成功的渗透和攻击过程，包含了复杂的信息搜集、攻击尝试、控制跳板、移动提权、信息回传过程。在这个过程中，极其容易出现信息输入方式不同于正常输入，数据包特征和网络行为特征存在差异，产生非必要的流量等异常行为。

有经验的安全专家极可能从这些异常行为中熟练地分析出数据攻击行为，但是却无法及时处理海量的流量数据。传统设备虽然可以持续分析流量，但是它们只是单纯地依赖特征库匹配进行机械式的拦截或者放行判断，不懂违规和异常行为的意义和逻辑，因此无法有效判断威胁，自然也

就无法有效保护隐私数据的安全。

因此，人们陷入两难的境地，如何将系统的不眠不休与安全专家的分析能力结合起来？安全态势感知依托大数据技术实现安全监测预警，可以完美地解决这个问题。安全态势感知以安全大数据为基础，从全局视角提升对安全威胁的发现识别、理解分析、响应处置能力，最终进行决策与行动，实现保护隐私数据安全不被侵犯的目的。

目前，网络安全态势感知大致可以分为态势认知、态势理解和态势预测三个阶段，态势认知主要是了解当前网络安全状态，态势理解主要是评估系统损失、溯源分析和取证分析，态势预测则是对态势发展情况的预测评估，比如态势跟踪和情境推演。态势感知阶段主要从以下三个方面来预测网络安全威胁的发生，保护隐私数据安全。

1. 感知资产脆弱性

网络安全脆弱性是网络攻击者入侵网络窃取隐私数据的重要入口，主要包括资产漏洞和弱密码配置不当。如果出现资产漏洞和不合理的配置，资产安全加固和防护措施难以进行，网络攻击者窃取隐私数据的概率大大增加。

对于资产漏洞，网络安全态势感知基于已知的漏洞信息，采用端口探测等手段，对网络中指定的主机、网络设备等资产进行漏洞检测，发现网络资产存在的漏洞；对于不合理的安全配置，网络态势感知采用基线安全配置检测工具，深度获取主机、服务器和网络设备等资产的配置信息，并与配置基线进行比较，发现资产配置的脆弱性。最终，根据发现的资产脆弱性，分析攻击者可能的攻击路径，采取有针对性的防护措施，减少攻击者进入信息系统窃取隐私信息的概率。

2. 感知安全事件

随着网络技术的发展，病毒、蠕虫、后门和木马等网络攻击的方式层出不穷，给用户的隐私数据造成极大的安全威胁，逐渐受到人们关注。为了保证网络系统的安全运行，保护隐私数据安全，网络中广泛使用了防火墙、入侵检测系统、漏洞扫描系统和安全审计系统等安全设备。这些安全设备会产生大量违反安全策略和安全规则的告警事件。但是，这些安全告警事件信息中含有大量的重复报警和误报警，且各类安全事件之间分散独立，缺乏联系，无法给安全管理员提供在攻击时序上和地域上真正有意义的指导，自然，防护隐私数据安全的能力也就有所欠缺。

但在真正窃取隐私数据的攻击中，大部分的安全告警事件并不是孤立产生的，它们之间存在一定的时序或因果联系。网络安全态势感知结合安全告警事件的运行环境，对原来相对孤立的低层网络安全事件数据集进行关联整合，并通过过滤、聚合等手段去伪存真，发掘隐藏在这些数据之后的事件之间的真实联系，提高信息系统应对网络攻击的能力，从而保护隐私数据。

3. 感知网络威胁

大数据时代，隐私数据窃取攻击行为逐渐呈现分布化、远程化与虚拟化等趋势，各类高危漏洞、0Day 漏洞使攻击特征库的及时更新与长期维护面临巨大困难，传统基于对攻击行为进行特征识别与比对的威胁感知和甄别机制，受到了来自新型攻击手法的巨大挑战。此外，传统的威胁检测手段在应对 APT 攻击时显得力不从心，因为传统的检测手段主要针对已知的威胁，对未知的漏洞利用、木马程序、攻击手法无法进行检测和定位。

面对层出不穷的网络攻击和新的数据安全威胁，网络安全态势感知从“知己”和“知彼”两个方面保障系统内隐私数据的安全。“知己”是采集

内部网络流量数据、日志数据和安全数据等，进行基于大数据分析、人工智能技术的异常行为检测，发现隐藏在海量数据中的网络异常行为；“知彼”方面是通过监测、交换和购买等各种方式，搜集恶意样板 Hash 值、恶意 IP 地址、恶意域名、攻击网络或者主机特征、攻击工具、攻击战技术、攻击组织等网络威胁情报数据，用于支撑安全运行维护、安全检测分析和安全运营管理，从整体上提高了信息系统应对新型网络威胁的能力。

网络安全态势感知技术综合各方面的安全因素，从整体上动态反映信息网络安全状况，并对信息系统安全的发展趋势进行预测和预警。借助网络安全态势感知，多方位采取应对措施，保护隐私数据的安全。比如网络监管人员可以及时了解网络的状态、受攻击情况、攻击来源以及哪些数据易受到攻击等情况，对将发起攻击的网络采取安全措施；网络用户可以清楚地掌握所在网络的安全状态和趋势，做好相应的防范准备，避免和减少网络中病毒和恶意攻击带来的损失；应急响应组织也可以从网络安全态势中了解所服务网络的安全状况和发展趋势，为制定有预见性的应急预案提供基础。

未来，大数据技术特有的海量存储、并行计算、高效查询等特点，将为大规模网络安全态势感知技术的突破创造机遇，借助大数据分析，对成千上万的网络日志等信息进行自动分析处理与深度挖掘，对网络的安全状态进行分析评价，感知网络中的异常事件与整体安全态势，保护隐私数据安全。

除了大数据与新技术的结合，还要保证隐私数据应用流程的透明化。现阶段，大数据处理技术大都表现神秘，比如大数据预测、数据库变化以及运算法则都是黑盒子不透明、不可追踪以及不可解释的状态，这些使得公众对个人隐私的控制权被严重削弱，信息控制者对信息的垄断控制不断加强。

在未来，可以将个人隐私保护理念融入技术架构的设计中，设置个人隐私保护原则，增强企业处理、利用个人信息各环节的透明度，在各个环

节进行隐私数据风险评价，并将风险评价告知信息主体，让信息主体自行决定是否继续或者删除自己的数据，增进用户参与，延伸用户控制。此外，还应丰富个人隐私权的内容。除传统的个人隐私权所覆盖的个人隐私决定权、查询权、更正权、补充权、封锁权、删除权、保密权之外，在技术成熟能提供相应支持时，赋予个人隐私被遗忘权与信息的可携带的权利。

公共部门也要充分意识到隐私保护的重要性，这既是对公民权益负责，避免自身的侵权责任，也是为了起到更好的社会垂范作用。只有公共部门明确隐私保护的意识、守住底线，才能更好地推动相关法规的完善和执行，让隐私保护成为整个社会的习惯。

在国家的监管和政策方面，除了希望能在建立相对完善的法律制度与保护机制，也希望我国的传统隐私保护模式做出改变，推动传统隐私权保护的与时俱进。因此，构建一部成熟完善的个人隐私保护法，是我国在大数据背景下保护隐私的必然趋势。这部立法应该定位为一部个人隐私权保护的立法，一部信息控制者、处理者合法使用大数据处理数据活动的保护法。个人信息的保护应分级分类，认识到“可识别的信息”与个人隐私保护基本原则适用间的相关性。着重对滥用数据信息的行为进行规制，强化对敏感信息的保护。

另外，大数据时代个人法律对隐私的保护也需转变思路。在未来，法律对个人隐私的保护应更多地关注信息处理、信息使用行为可能引发的风险，而不是仅仅将重心聚焦在是否通过正常途径采集信息的行为上，强调让信息控制者、处理者承担责任。传统框架以个人信息定义作为法律适用的前提与边界，但大数据时代个人信息边界日益模糊。虽然个人隐私的概念非常重要，不能摒弃，但我们需要突破对个人隐私定义的路径依赖，重视对使用环节的规制。因为大数据环境下个人隐私保护的风险并非源于个人隐私信息收集之初，而是出自具体的使用环节。当然，关注重心与焦点的转移并不意味着忽视信息采集的环境，只是规制的重心应放在个人信息的处理、利用引发的不合理风险与问责机制方面。

法律是隐私保护的坚实后盾，但这需要我们善用这后盾来保护自己，当个人隐私受到侵犯时，应当做到积极寻求途径进行维权，从而保证自己的合法权益不受侵犯。我们要积极采取协商、调解的方式来应对侵犯隐私权的问题，在必要的时候还要采取诉讼手段维护自己的合法权益。

此外，人才是确保数据安全的关键因素。相较于国外，我国大数据技术起步较晚，且在发展过程中存在相对明显的断层，因此大数据保护的综合性人才短缺。未来大数据人才培养要立足于我国的人才需求，参考国外大数据人才培养模式，加快实施有针对性的大数据人才培养计划。通过建立相关的大数据实验环境和平台整合交叉学科和交叉领域的知识，通过完整的培训体系培养大数据人才的全局观、大局观、安全观，既可以自顶向下地通过业务探索数据背后蕴含的商业价值，又可以自底向上地去实现数据获取、数据挖掘以及数据决策的全流程，并且在实现数据价值的过程中注重数据的安全保护，以适应大数据时代的发展。

无论在哪个时代，数据本身是无罪的。我们只能用制度和规则来规范对网络平台用户数据的使用，使之在法律和道德的框架之内有序运行。明确用户的隐私数据，哪些可以用，哪些可以怎么用，根据不同人对隐私的理解做出分类处理，保证数据的合理应用，这样才能保证网络行为数据这一由大众产生出的宝藏最终服务于增进大众的福祉、促进人类进步。

参考文献

[1] 杨义先，钮心忻. 安全简史. 电子工业出版社，2017.

[2] 范渊. 智慧城市与信息安全（第 2 版）. 电子工业出版社，2016.

[3] 工业和信息化部电信研究院. 中国大数据发展调查报告，2017.

[4] 周苏，王文. 大数据导论. 清华大学出版社，2016.

[5] 方滨兴，贾焰，李爱平，等. 大数据隐私保护技术综述. 大数据，2016（1）.

[6] 德勤有限公司 .2017 亚太区隐私与个人信息保护白皮书，2017.

[7] 童拿云. 大数据时代的个人隐私保护. 上海师范大学硕士学位论文，2015.

[8] 龙媛. 论信息时代的网络隐私权保护. 世纪桥，2010（11）.

[9] 王海珍. 未来，如何安放我们的隐私. 中华儿女，2016（9）.

[10] 刘鹏，王丽萍. 信息时代隐私权保护面临的挑战与应对，政法论丛，2008（6）.

[11] 中国青年政治学院互联网法治研究中心，封面智库. 中国个人信息安全和隐私保护报告，2016.

[12] 新华每日电讯. “互联网 + 医疗”来临就医方式将如何转变，2015-4-28.

[13] 李广建，化柏林. 大数据时代：新思维与管理. 中国人事出版社，2016.

[14] 赵伟. 大数据在中国. 文艺出版社，2014.

[15] 高扬，卫峥，尹会生. 白话大数据与机器学习. 机械工业出版社，2016.

[16] 刘雅辉，张铁赢，靳小龙，等. 大数据时代的个人隐私保护. 计算机研究与发展，2015（1）.

[17] 徐素芹. 我国网络环境下隐私权法律保护初探. 天津市政法管理干部学院学报，2009（4）.

[18] 张晓娟，王文强，唐长乐. 中美政府数据开放和个人隐私保护的政策法规研究. 情报理论与实践，2016，39（1）.

[19] 中国商业联合会数据分析专业委员，中国大数据人才培养体系标准，2017.

[20] 谷安天下 . 国外个人敏感信息与隐私保护法律实践，2017.

[21] 360 企业安全研究院 . 走进安全，网络世界的攻与防，2018.

[22] 冯登国，张敏，李昊. 大数据安全与隐私保护. 计算机学报，2014，37（1）.

[23] 曹珍富，董晓蕾，周俊，等. 大数据安全与隐私保护研究进展. 计算机研究与发展，2016（10）.

[24] 围密. 手机 App 隐私泄露，谁是真正的“元凶”，https://www.sohu.com/a/225038739_100071868.

[25] 襄阳日报. App 信息泄露，安装时你注意“权限”了吗，https://baijiahao.baidu.com/s?id=1610317236107922758&wfr=spider&for=pc.

[26] 龙泉驿检察. 手机 App 泄露隐私，你还亲手点了“同意”？安装 App 时别忘了这一步，http://dy.163.com/v2/article/detail/D66K1Q9M0514LJQR.html.

[27] 刘驰，胡柏青，谢一. 大数据治理与安全：从理论到开源实践. 机械工业出版社，2017

[28] 本·斯派维，乔伊·爱彻利维亚著，赵双，白波译. Hadoop 安全. 人民邮电出版社，2017.

[29] 潘晓，霍峥，孟小峰 . 位置大数据隐私管理. 机械工业出版社，2017.

[30] 特雷莎·M. 佩顿，西奥多·克莱普尔著，郑淑红译. 大数据时代的隐私. 上海科学技术出版社，2016.

[31] 特伦斯 . 克雷格，玛丽·E. 卢德洛芙著，赵亮，武青译. 大数据与隐私. 东北大学出版社，2016.

[32] 马克尔·杜甘，克里斯托夫·拉贝著，杜燕译. 赤裸裸的人——大数据，隐私和窥视. 上海科学技术出版社，2017.

[33] 中国科协学会学术部. 大数据时代隐私保护的挑战与思考. 中国科学技术出版社，2015.

[34] 约翰·帕克著，关立深译. 全民监控：大数据时代的安全与隐私困境. 金城出版社，2015.

[35] 王忠. 大数据时代个人数据隐私规制. 社会科学文献出版社，2014

[36] 茱莉亚·霍维兹，杰拉米·斯科著，董淼译. 无处安放的互联网隐私. 中国人民大学出版社，2017.

[37] 尤夫娜·霍夫施泰特著，陈巍译. 大数据之眼：无所不知的数字幽灵. 浙江文艺出版社，2018

[38] 孔令杰. 个人资料隐私的法律保护. 武汉大学出版社，2009.

[39] 布莱恩·克雷布斯著，曹烨，房小然，译. 裸奔的隐私. 广东人民出版社，2016.

[40] 宋进，唐光亮. 网络安全态势感知技术研究与应用. 通信技术，2018，51（6）.