中国信息协会
信息安全专业委员会

每日经济新闻
NATIONAL BUSINESS DAILY

19th Asian Games
Hangzhou 2022

杭州2022年第19届亚运会官方合作伙伴
Official Prestige Partner of the 19th Asian Games Hangzhou 2022

安恒信息官方微信

西湖论剑2012-2022

个人信息与隐私保护白皮书

2022

西湖论剑10周年系列白皮书

中国信息协会信息安全专业委员会
每日经济新闻
安恒信息

目录
CONTENTS

个人信息安全
与隐私保护相关法规现状

1 个人信息安全现状概述

随着信息化与经济社会持续深度融合，网络已成为生产生活的新空间、经济发展的新引擎、交流合作的新纽带。截至2020年12月，我国互联网用户已达9.89亿，互联网网站超过443万个、应用程序数量超过345万个，个人信息的收集、使用更为广泛。

国务院《“十四五”数字经济发展规划》指出，数字经济成为继农业经济、工业经济之后的主要经济形态，发展数字经济是国家的重要战略部署，2035年我国数字经济将迈向繁荣成熟期，形成统一公平、竞争有序、成熟完备的数字经济现代市场体系，数字经济发展基础、产业体系发展水平将位居世界前列。

云计算、5G、工业互联网、车联网、物联网、大数据等新兴技术快速推进数字化发展进程，加速挖掘个人信息数据价值，让人们充分享受数字化所带来的诸多便利。但随着数据价值的发掘，个人信息的安全性也面临着由个人信息数字化所带来的风险。当重要数据被数字化后，能得到快速、有效利用的同时也面临着更加容易被窃取、破坏的风险，传统的物理防护措施面对数字化的发展大潮已无能为力，如何保护个人信息已然成为现代社会所面临的挑战。

近年来我国个人信息保护力度不断加大，打击机构、企业、个人对个人信息的非法收集、获取、使用、买卖等行为。但在现实生活中，还存在因商业利益随意收集、违法获取、过度使用、非法买卖个人信息的情况，利用个人信息侵扰人民群众生活安宁、危害人民群众生命健康和财产安全等问题。在数字化时代，个人信息保护已成为广大人民群众最关心最直接最现实的利益问题之一，也是一个全球性的合法合规问题。

2021年，公安部网安局坚决贯彻落实上级单位的指示要求，深入推进“净网2021”专项行动，针对人民群众急难愁盼的个人信息保护问题，全力组织开展侦查打击工作。全国公安机关全年共破获侵犯公民个人信息案件9800余起，抓获犯罪嫌疑人1.7万名。

2 个人信息与隐私的关系

个人信息的概念

个人信息是指与特定个人相关联的、反映个体特征的具有可识别性的符号系统，包括个人身份、工作、家庭、财产、健康等各方面的信息。

一般认为，个人信息的概念始于1968年联合国“国际人权会议”中提出的“资料保护”。最早的个人信息保护立法是1970年德国黑森州制定的《个人资料保护法》；最早的国家级个人信息保护立法则是1973年瑞典国会颁布的《资料法》。

对我国而言，依据《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第一条规定，“刑法第二百五十三条之一规定的‘公民个人信息’，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特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。”

自2021年11月1日正式施行的《中华人民共和国个人信息保护法》（以下简称“个人信息保护法”）指出，个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

个人信息与隐私的关系

我们通常所说的窃取个人信息，有极大一部分都属于侵害个人隐私行为。

2021年施行的《民法典》指出，自然人享有生命权、身体权、健康权、姓名权、肖像权、名誉权、荣誉权、隐私权、婚姻自主权等权利。法人、非法人组织享有名称权、名誉权和荣誉权。

隐私权在法律上的定义为，公民享有的私人生活安宁与私人信息依法受到保护，不被他人非法侵扰、知悉、搜集、利用和公开等的一种人格权。按照通常说法，即是指“私生活不受干涉的权利”，“私人信息未经允许不得公开的权利”。也就是说，每一个人均有“不受旁人侵扰的权利”。隐私权的实质在于，个人可以自由地决定何时、何地以何种方式与外界沟通。从这个方向来讲，隐私权表现为个人对自身的支配权。

基于法律属性，隐私权主要是一种精神性的人格权，隐私主要体现的是人格利益，侵害隐私权也主要导致的是精神损害。而个人信息权在性质上属于一种集人格利益与财产利益于一体的综合性权利，并不完全是精神性的人格权，其既包括了精神价值，也包括了财产价值。另外，隐私权是一种消极的、防御性的权利，在该权利遭受侵害之前，个人无法积极主动地行使权利，而只能在遭受侵害的情况下请求他人排除妨害、赔偿损失等。而个人信息权则并不完全如此。权利人除了被动防御第三人的侵害之外，还可以对其进行积极利用。

隐私权制度的重心在于防范个人秘密不被非法披露，并不在于保护这种秘密的控制与利用；对个人信息权的侵害主要体现为未经许可而收集和利用个人信息、侵害个人信息，主要表现为非法搜集、非法利用、非法存储、非法加工或非法倒卖个人信息等行为形态。其中，大量侵害个人信息的行为都表现为非法篡改、加工个人信息的行为。

3 国外个人信息安全与隐私保护相关法规现状

国际上个人信息保护的立法原则

在欧洲，以德国为代表的大陆法系国家，将个人信息视作公民人格和人权的一部分，认为个人信息是自然人人格的载体，沿用一般人格权的保护思路引入“信息自决权”。以美国为代表的海洋法系国家，形成思想更多地基于生活中的公序良俗，将个人信息视作公民隐私和自由的一部分，沿着隐私保护的思路提出“信息隐私权”概念。

1973年，美国健康、教育和社会福利部首次提出了《公平信息实践》，构成了全球个人信息保护的思想渊源与基本框架。此后，《关于保护隐私和个人信息跨国流通指导原则》中提出了个人信息保护八大原则。

这些原则经过40余年的发展演变和提炼，最终演变为五大国际原则：公开性原则、限制性原则、数据质量原则、责任与安全原则、个人信息权利保护规则，由他们共同作为各国和国际组织制定个人信息保护政策的基础。

欧盟个人信息安全与隐私保护法规现状

欧盟对于个人信息的隐私权保护可以说是世界上最为全面和严格的。1995年，欧盟通过经典的《个人数据保护指令》，该法律源于美国早期的FIPs原则，根本而言，欧盟强调的个人信息保护，从民法上讲就是基于信息自主、信息控制和信息自决。

为应对云计算、大数据、移动互联网及跨境数据处理等应用场景所带来的新挑战，2018年，新的数据保护法案《通用数据保护指令》（GDPR）生效。GDPR旨在加强欧盟区居民的数据保护，特别是对儿童信息使用和准许的保护，并且在数据安全方面提供更加坚实的框架，指导跨欧盟个人数据的商业使用。此外，该指令还包括广泛的与隐私相关的要求。GDPR自发布后即成为全球数据保护的最严标准，被视作大数据监管新时代的标志，对于国际间的数据流动引入了新的职责和限制。

对个人敏感信息的界定，GDPR将涉及以下一种或一种以上类别的个人数据视为敏感数据：种族或民族出身、政治观点、宗教/哲学信仰、工会成员身份、涉及健康、性生活或性取向的数据、基因数据、经处理可识别特定个人的生物识别数据。同时，GDPR对从个人信息的采集，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：

事前，在个人信息的采集环节，需要实行“最少采集”原则，并且采集之后只能用于特定目的。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，要在一定期限后予以销毁。

事中，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。

事后，有相应的法律责任的追究和法律救济渠道。除了进行罚款，很多国家对违反法律泄漏个人信息是可以处以刑事责任。

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及企业的个人信息泄露采取法律制裁。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。2019年7月8日，英国信息监管局发表声明称英国航空公司因为违反《一般数据保护条例》被罚1.8339亿英镑。

对于个人信息数据的跨境传输，GDPR中有三种主要的保障机制：“充分性认定”程序、标准合同条款（SCC）以及“具有约束力的公司规则（BCRs）”。“充分性认定”程序即确保第三国的数据保护标准与欧盟标准相当，截至目前，全球已有13个国家通过欧盟“充分性认定”程序。

美国个人信息安全与隐私保护法规现状

美国是世界上最早提出并通过法规对隐私权予以保护的国家，美国在1974年通过《隐私法案》（PrivacyAct），1986年颁布《电子通讯隐私法案》，1988年又制订了《电脑匹配与隐私权法》及《网上儿童隐私权保护法》。

对于个人信息保护，美国的策略较为灵活主要采取行业自律模式，同时，美国也以分散立法的形式对该模式予以补充，如《联邦贸易委员会法》适用于线下和线上的隐私和数据安全，《儿童网上隐私保护法》《电子通讯隐私法案》《金融服务现代化法》《健康保险流通与责任法》等行业立法也为特定行业的隐私保护或特定类型的敏感信息保护提供了法律依据。

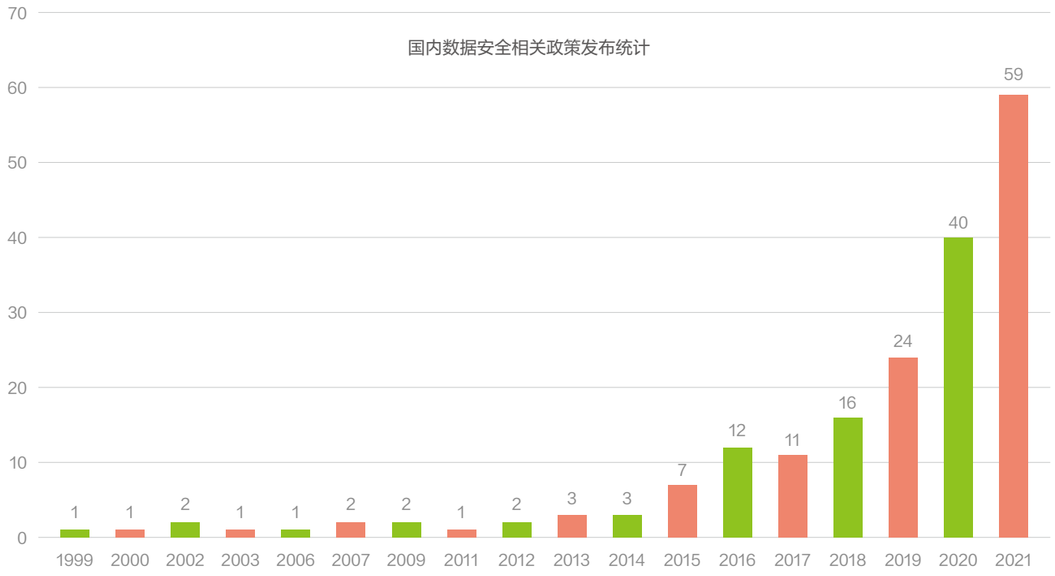
2018年5月25日，关于个人数据保护的欧盟新一代制度规范《一般数据保护条例》（GDPR）正式施行。随后，美国以及美国各州陆续实施了个人信息保护相关的法律法规，《加州消费者隐私法案》（CCPA）于2018年6月28日通过，并于2020年1月1日起正式施行。除了CCPA，各个州也颁布了其相应的隐私法案，例如2021年7月颁布的《科罗拉多州隐私法案》（CPA）以及弗吉尼亚消费者数据保护法案（VCDPA)。

此外，在法律救济方面，基于美国的行业自律模式，除美国联邦及州级政府提起诉讼外，公司还面临用户及投资人提起民事诉讼的风险。2017年6月，美国最大保险公司AnthemInc.在发生8000万客户个人数据泄露事件后，就曾签署过一份1.15亿美元的和解协议，同意向每位原告支付235美元的赔偿，而遭受最大伤害的诉讼集体将获得高达10000美元的赔偿。

4 国内个人信息安全与隐私保护相关法规现状

数据安全法律法规与政策体系不断完善

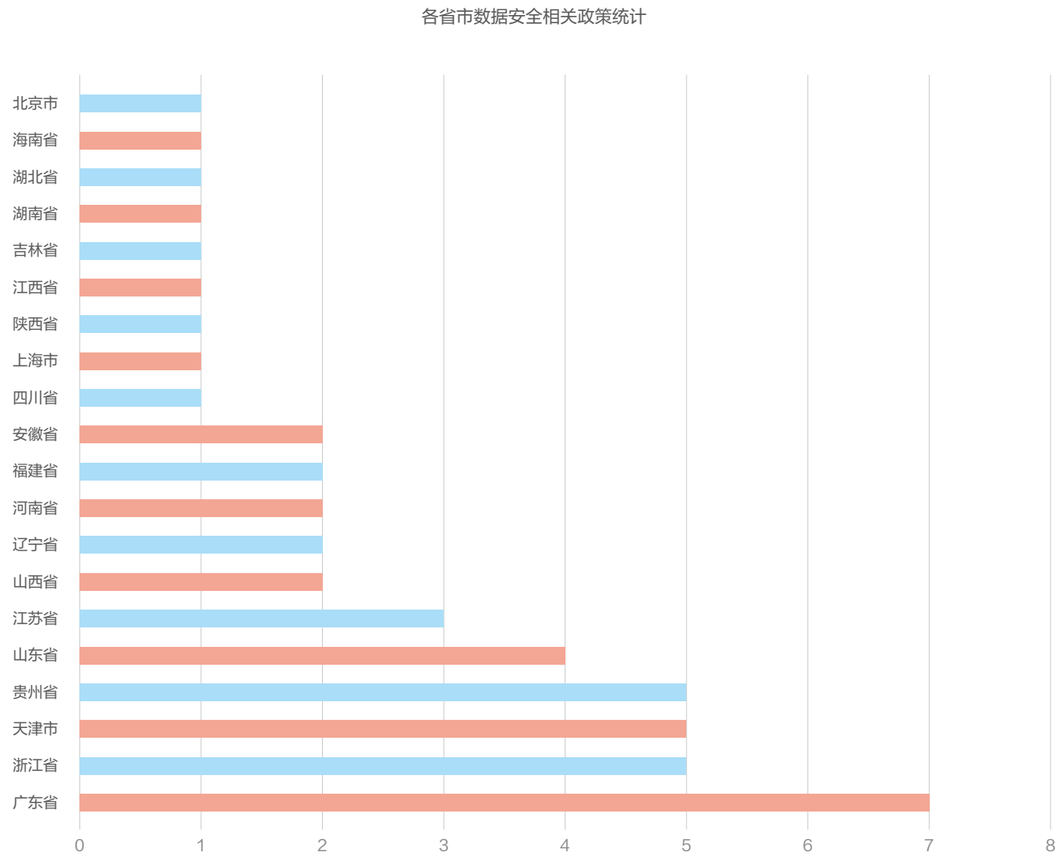
2021年被称为中国的“数据安全元年”，《 中华人民共和国数据安全法 》（ 以下简称“数据安全法”）《 个人信息保护法 》等法律法规密集出台，加之2017年实施的《 中华人民共和国网络安全法 》（ 以下简称为“网络安全法”），“三法并行”构成国内网络空间治理和数据保护的法律底座。



90年代末，我国开始了数据安全方面的建设，相关政策开始出现并实施，其后，“十三五”规划指出：“牢牢把握信息技术变革趋势，实施网络强国战略，加快建设数字中国，推动信息技术与经济社会发展深度融合，加快推动信息经济发展壮大。”2016年到2020年的“十三五”期间，数据安全政策出台频率明显增加，数据安全整体政策环境趋于完善，数据安全领域的相关市场加速成型。

2017年6月1日，《 网络安全法 》施行，2021年，《 民法典 》《 数据安全法 》《 个人信息保护法 》相继施行，标志着我国以数据安全保障数据开发利用和产业发展全面进入法治化轨道，重要数据及个人信息保护成为时代需求。

“十四五”规划继续推动数字中国建设，2021年作为“十四五”的开局之年，出台数据安全相关政策数量高达59项，为数据安全产业的发展夯定了更坚实的政策基础。安全是发展的前提，发展是安全的保障，高频率的数据安全政策出台，制定了各参与方获取、使用数据的界限，加强了数据的安全，保障国家数字化产业的健康发展。



从地方维度看，广东省在数据安全立法方面，出台相关政策最多，其次是浙江省、贵州省、山东省、江苏省、山西省等地区。随着《 网络安全法 》的发布及“十三五”规划，地方性政策的发布时间主要集中在2019年、2020年和2021年。随着数字化的发展，根据相关政策的通知，不难得出，在未来几年内，各省份、直辖市等地区将会陆续出台更多地方性数据安全相关政策，以更好的进行数据的标准化及等级划分，以保障地方在数据要素市场化以及数字化转型过程中数据的安全性。

数据分类分级及重要数据界定不断明确

随着《数据安全法》以及《个人信息保护法》的颁布及施行，首要思考的是，关于其中提到的数据、重要数据、个人信息、个人敏感信息等名词应如何进行划分，又应该如何在具体的企业组织活动中使数据安全管理行之有效。2021年12月17日，中央网信办网络数据管理局副局长方新平在“2021啄木鸟数据治理论坛”中称：“数据安全法、个人信息保护法的施行，标志着我国数据安全和个人信息保护工作迈入了新阶段。”

目前中央网信办正在抓紧制定数据安全法、个人信息保护法配套法规规章。比如正在起草的《网络数据安全管理条例》《数据出境安全评估办法》《个人信息出境标准合同规定》《人脸识别技术应用安全管理暂行规定》，以及数据安全、个人信息保护的合规审计制度和相关标准规范。

2022年1月13日，全国信息安全标准化技术委员会发布《信息安全技术重要数据识别指南》（征求意见稿），其中对“重要数据”进行了较此前更为明确的范围界定。

“重要数据”的概念首次在2016年11月发布的《网络安全法》中提出，法律中对重要数据的某些跨境传输、特别安全保护义务提出了具体要求。2017年4月，国家互联网信息办公室在《个人信息和重要数据出境安全评估办法（征求意见稿）》中明确了重要数据的范围，即“指与国家安全、经济发展，以及社会公共利益密切相关的数据”。此外，《指南》征求意见稿中明确说明“基于海量个人信息形成的统计数据、衍生数据”，例如基于海量用户个人信息形成的市场趋势判断、市场喜好判断等，有可能属于重要数据。

《数据安全法》中对数据分类分级保护制度及重要数据目录的建立作出明确规定：“国家建立数据分类分级保护制度，国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。”

中国的数据保护、网络安全相关立法正处于逐步完善的进程当中，且相应的国家标准也正处于同步制定的阶段。在未来不久，针对各行业的重要数据界定标准及数据分类分级标准不时将会推出，中国将逐步迈进到数据有效化，标准化，合法安全利用的大数据时代，形成统一公平、竞争有序、成熟完备的数字经济现代市场体系。

国内个人安全与隐私保护相关法律法规

《数据安全法》第二条指出，在中华人民共和国境内开展数据处理活动及其安全监管，适用本法；同时第三条对数据进行了界定：“本法所称数据，是指任何以电子或者其他方式对信息的记录。数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。”那么，对个人信息的数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等亦属于数据处理的一部分。

《个人信息保护法》于2021年8月20日通过，2021年11月1日起施行，这是我国第一部个人信息保护方面的专门法律，旨在保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，本法共分为八章六十四条，其中对个人信息、敏感个人信息等作出了明确定义：

个人信息

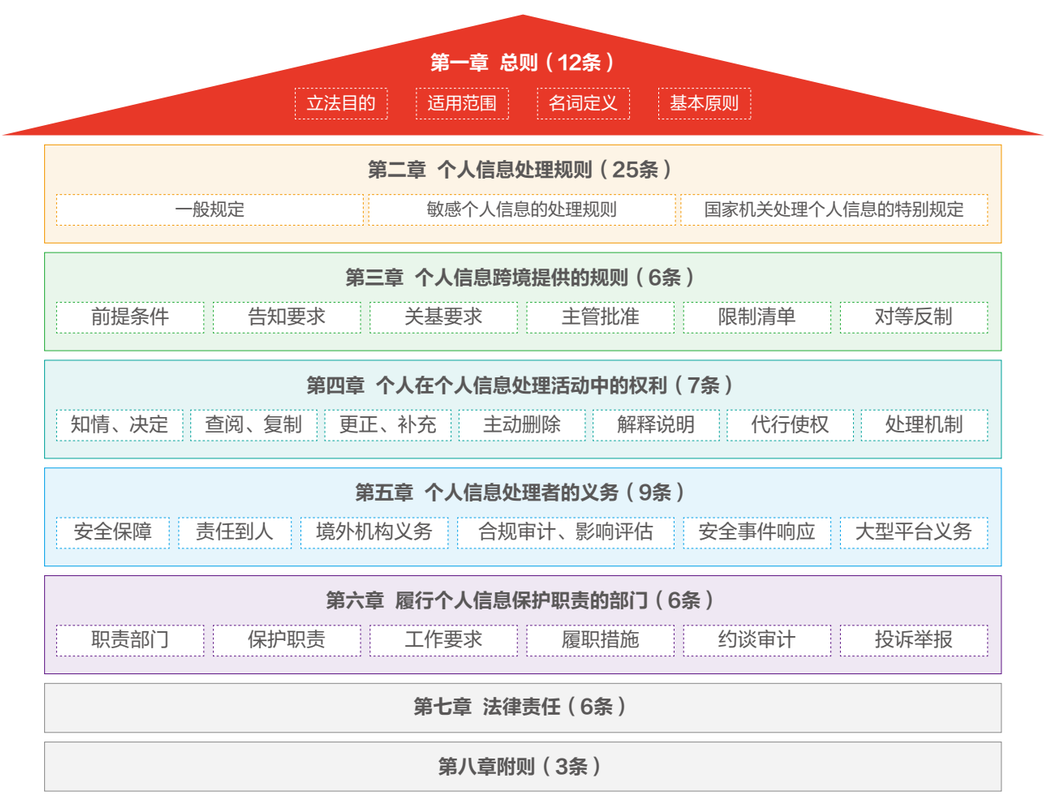
是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

个人信息的处理

括个人信息的收集、存储、使用、加工、传输、提供、公开等。

敏感个人信息

一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。



个人信息保护法结构

法条中主要对以下事件进行了限制：

禁止大数据“杀熟”

【第二十四条】个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。

个人可以拒绝强制推送个性化广告

【第二十四条】通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。

限制过度收集个人信息

【第六条】处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。

【第十条】任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

规范采集公共场所人脸识别

【第二十六条】在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。

个人有权撤回处理个人信息

【第十五条】基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。个人撤回同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

规范未成年人个人信息保护

【第三十一条】个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。 个人信息处理者处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则。

限制敏感个人信息处理

【第二十八条】只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。

【第二十九条】处理敏感个人信息应当取得个人的单独同意；法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。

规定逝者个人信息处理

【第四十九条】自然人死亡的，其近亲属为了自身的合法、正当利益，可以对死者的相关个人信息行使本章规定的查阅、复制、更正、删除等权利；死者生前另有安排的除外。

禁止企业组织在个人不同意提供个人信息时拒绝服务

【第十六条】个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外。

对于违反《个人信息保护法》所负的法律责任，法条中作出了如下规定：

惩罚力度	违法行为	处置说明	企业	相关责任人
一般违法	违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的	由履行个人信息保 护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务	拒不改正的，并处一百万元以下罚款	处一万元以上十万元以下罚款
情节严重	有前款规定的违法行为，情节严重的	期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人	· 没收违法所得 · 并处五千万元以下或者上一年度营业额百分之五以下罚款 · 责令暂停相关业务或者停业整顿 · 吊销相关业务许可或者吊销营业执照	处十万元以上一百万元以下罚款
记入信用档案并予以公示	有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。			
给予处分	国家机关不履行本法规定的个人信息保护义务的，由其上级机关或者履行个人信息保护职责的部门责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。			
民事责任	· 个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任； · 损害赔偿责任按照个人因此受到的损失或者个人信息处理者因此获得的利益确定； · 难以确定的，根据实际情况确定赔偿数。			
刑事责任	侵害众多个人的权益的，人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。			
	· 违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚； · 构成犯罪的，依法追究刑事责任。			

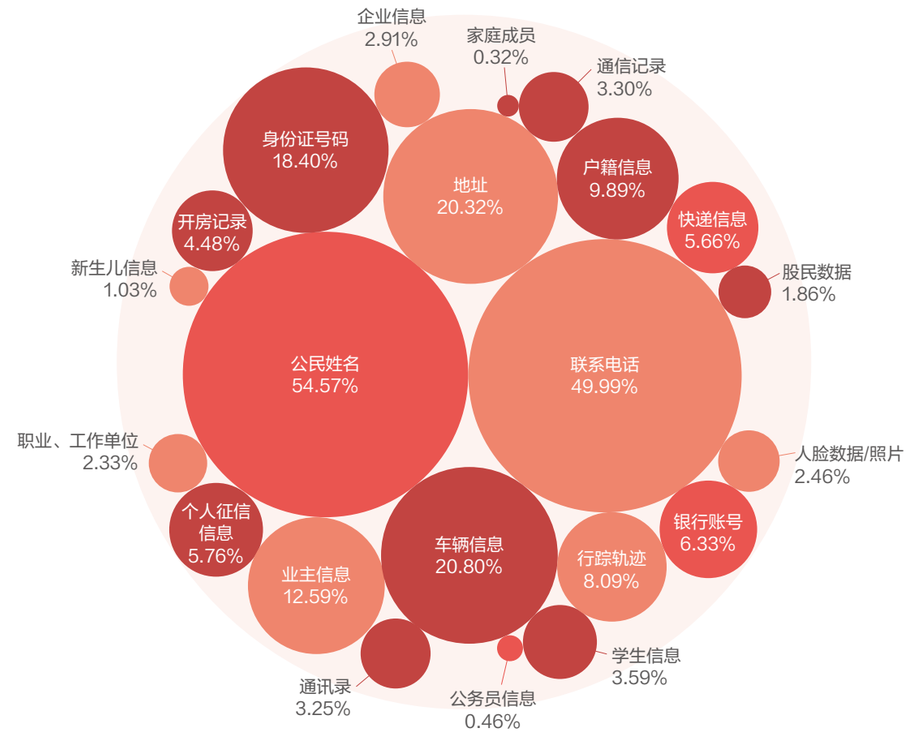
个人隐私保护现状

1 个人信息与隐私保护现状分析

违法侵犯公民个人信息问题严重

近年来，随着互联网特别是移动互联网蓬勃发展，丰富多样的应用形态已深入社会生产、人民生活的方方面面，在带来诸多便利的同时，也暴露出一些违规收集使用个人信息、不合理索取用户权限等侵害用户权益的突出问题。据《浙江省互联网发展报告》显示，仅2017年，浙江有72.8%的网民经历过个人信息泄露。有研究员在裁判文书网上获取了8602份与侵犯个人信息相关的判决书，以分析近年来个人隐私保护现状，其结果显示有如下特征：

个人数据泄露涉及面广，多用于诈骗牟利活动



个人信息泄露类型

分析显示，在判决书中涉及的个人信息中，姓名及联系方式占比最多，紧随其后的是身份证信息、居住地址和车辆信息。其中值得注意的是，在泄露的车辆信息中，20.79%的居住地址则主要从房地产公司和快递公司泄露。此外，部分涉案数据针对特殊群体，如新生儿和股民。此类数据往往直接从相关从业者手中流出，买家购买数据的主要诉求通常是有针对性的推销或是诈骗。

例如，2019年8月1日，江苏省常熟市市场监督管理局在执法检查中发现，江苏省常熟市某美容馆（月子中心）为拓展经营业务，向杨某购买在常熟市建卡和分娩的孕产妇个人信息，并通过微信联系客户拓展业务。经查，自2017年5月起，该美容馆违法购买的消费者个人信息包括孕产妇姓名、孩子姓名、孩子性别、分娩日期、分娩医院、分娩方式、联系方式、户口住址、产后休养地址等，共计36741条。

在研究所分析的8602份文书中，有6949份提到了被告在获得数据后的用途。而在一份文书中，可能出现多个被告，因此数据可能会有多种用途。其中，大部分被告选择直接贩卖数据贩卖牟利，占比79.77%。此外，34.36%被用于推广，10.48%则和诈骗相关。

由此可见，对公民个人来说，对个人信息的侵犯可能会招致诈骗、推销等后果，严重者甚至会导致生命安全及财产安全受到危害。

2020年6月24日，某银行支行营业室在某幼儿师范学校千余名毕业生不知情的情况下，批量开立12536户Ⅱ、Ⅲ类电子账户，涉及1457名学生，平均每人名下近10个账户。据了解，崇左师专在2013年至2018年间与农行崇左江州支行开展代收学杂费、代发放奖助学金等方面合作。合作期间，学校把学生的身份证、姓名信息交给银行，由银行录入系统用于开展业务。

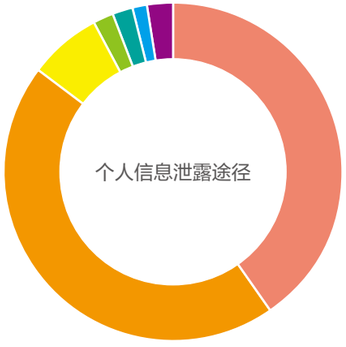
2022年1月20日中国人民银行南宁中心支行官网消息，某银行支行未落实个人银行账户实名制管理规定；违规使用个人金融信息；未严格落实银行账户风险监测要求；未按规定完整保存客户身份资料，故处以警告并共处人民币1142.50万元罚款。

2018年1月25日，浙江绍兴某高校在校生梁某因无力偿还网络借贷公司借款，自觉愧对父母，服用大量秋水仙碱自杀。该案属于大数据公司买卖个人信息与“套路贷”犯罪相互结合的新型案件。

经核查，上海显佳网络科技有限公司名为大数据信息分析公司，实际是通过研发借来花、掌上花等实际不能贷款的APP软件，骗取受害者注册APP时的个人信息：受害者在注册后，他们会用“审核不通过”等理由拒绝放贷。

获得信息后，公司会通过第三方公司形成风控报告，将公民个人信息贩卖给壹周金等网络贷款公司，贷款公司有了这些大数据信息，就可以精准地找到这些需要借贷的人。这些公司名为小额贷，实则变相的高利贷公司，大量公民个人信息泄露后，这些公司唯利是图，聘用社会闲散人员成立催收部，一旦用户欠款，便暴力催收，易滋生犯罪，产生严重后果。

贩卖个人信息来源多样，多来源于内部人员

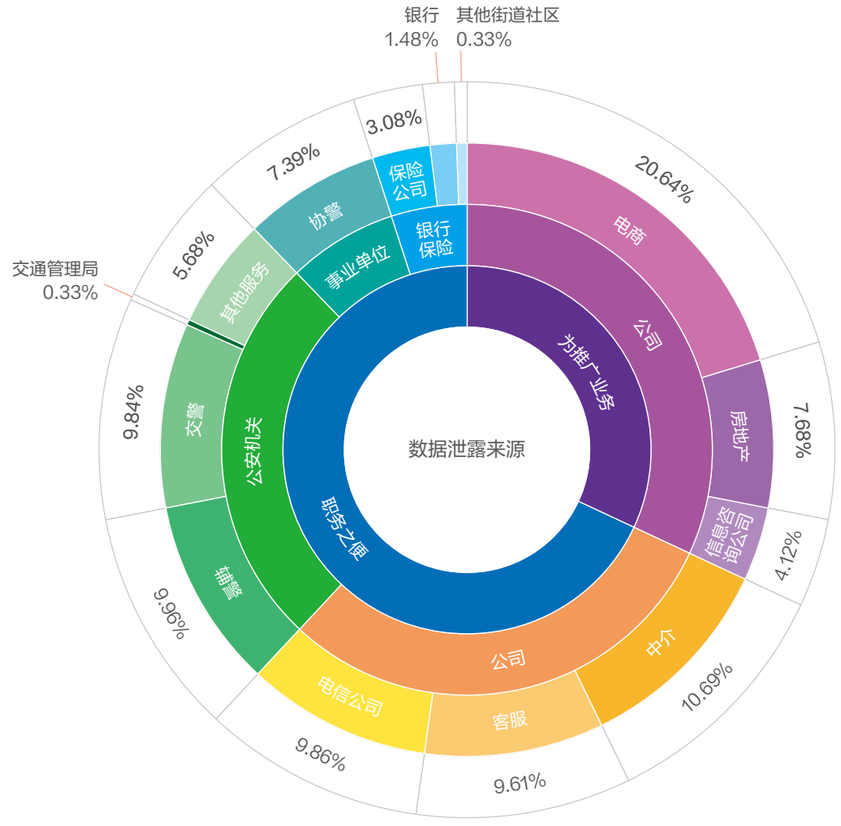


2017年，公安部网络技术研发中心主任许剑卓曾表示，行业内部人员已经成为侵犯公民个人信息犯罪的重要主体。他指出，从治理犯罪来说，打击源头是最重要的工作。而在2018-2020的“净网行动”中，公安机关抓获侵犯公民信息的行业“内鬼”3000余名，在“净网2021”专项行动中则抓获行业“内鬼”500余名。

谈及数据泄露，人们往往会将其与黑客行为划上等号，然而在实际社会活动中，有时候数据泄露的技术成本并不高，真正成为信息泄露主力的反而是行业内部人员，也就是俗称的“内鬼”。

据公安部网络安全局副局长钟忠称，“内鬼”监守自盗、内外勾结是公民个人信息泄露的一个重要原因。

在研究所获取的八千余份文书中，近四分之一的“内鬼”来自公安机关内部。一般而言，公安内部人员能接触到的敏感个人信息更多，诸如家庭住址、车辆、行踪轨迹、开房记录、犯罪记录等等。



数据显示，大部分“内鬼”从属于基层派出所和交警大队，这其中又以辅警和协警居多——虽然这些“编外人员”权限较低，但他们仍可以通过盗用正式干警的数字证书，或以用他们的账号密码登录公安内网等方式获取数据。此外，也有文书表明，有些干警是自己把数字证书权限交予“内鬼”的。

此外，涉及“内鬼”的信息往往与其所在行业有着强关联。房地产工作人员主要贩卖的是业主、小区信息，银行从业人员则“主营”股民、贷款和账户信息。而不同专业领域又涉及到不同的利益链条，导向了不同的犯罪类型。例如，从电信公司工作人员手中流出去的数据常被用于电信诈骗和推广，从各个渠道中流出的贷款相关数据则和网络放贷业务有关联。可以说，侵犯个人信息，是电信诈骗、敲诈勒索、盗刷信用卡、非法讨债、恶意注册账号等一系列违法犯罪的源头性犯罪，堪称“百罪之源”。

除“内鬼”外，通过购买、交换等方式获取公民个人信息的案件也不在少数，这说明公民个人信息的买卖市场仍然不容小觑，一条数据可能经手多人，被“多次利用”。其中，不少案例中的被告假借“信息咨询公司”之名从事个人信息买卖犯罪。另外，已查获的案件中，还有黑客利用技术手段窃取进行犯罪活动，黑客会利用网站、APP的技术漏洞，采取植入木马、病毒感染、撞库等技术手法，非法获取公民个人信息。

随着个人信息保护相关立法的不断完善，执法力度逐渐加强，2016年-2019年，全国惩处了多起侵犯个人信息相关事件，仅2019年，约惩处1865条。随后在2020年-2021年，事件数量逐年下降。

违法侵犯公民个人信息问题严重

近年来，随着国家大数据发展战略加快实施，大数据技术创新与应用日趋活跃，产生和集聚了类型丰富多样、应用价值不断提升的海量网络数据，成为数字经济发展的关键生产要素。与此同时，数据过度采集滥用、非法交易及用户数据泄露等数据安全问题日益凸显，做好网络数据安全管理尤为迫切。

来自国家互联网应急中心（CNCERT）的《APP违法违规收集使用个人信息监测分析报告》中指出，目前APP超范围收集个人信息的问题目前主要包括七种情形：

敏感权限声明超出必要范围

少量APP在未提供实际功能的情况下，仍然声明了相关敏感权限，存在热更新后调用和SDK（软件开发工具包）调用权限的风险。

权限索取超出必要范围

一些APP超出当前功能需要索取权限，例如某应用的电话拦截功能索要了短信、存储、通讯录等7项敏感权限，整改后只保留了功能实现所必需的3项敏感权限。

收集数据的敏感性超出必要范围

一些APP在使用低敏感性数据即可实现功能的情况下，仍然收集高敏感性数据。例如，普通的天气查询功能只需要城市或地区级的粗略位置信息，不应索要精准位置等敏感个人信息。

收集数据的具体内容超出必要范围

一些APP在仅需部分数据内容即可实现功能的情况下，却实际收集了全部内容。例如，查找好友功能只需匿名化后的手机号码即可实现功能，不应超范围收集通讯录联系人的姓名、邮箱、地址等内容。

收集方式超出必要范围

APP收集个人信息的方式包括单次读取、本地存储、上传云端等，对个人的影响程度依次递增，应在满足功能需求前提下选择影响程度最低的收集方式。例如，只需单次读取或本地存储即可实现功能，不应默认使用上传云端。

收集频率超出必要范围

有的APP收集每项个人信息的频率明显超出当前功能的必要范围，例如，某运动健身类应用在用户观看视频等无关功能时，每分钟获取位置信息近百次，明显超出必要范围。

收集场景超出必要范围

很多APP除了在功能必需的合理场景收集信息，还在启动、自启动、后台运行、使用不相关功能等其他场景收集信息，违反了必要原则。例如，某应用除了在共享位置时收集位置信息，还在扫码支付等不相关功能收集位置信息，可用于用户消费行为画像分析，近期已自行整改。

《信息安全技术个人信息安全规范》在第5.5款“个人信息保护政策”中明确，个人信息保护政策应公开发布且易于访问，例如，在网站主页、移动互联网应用程序安装页、交互界面或设计等显著位置设置链接。

如今，越来越多的APP开始使用弹窗这种“增强式告知”的方式向用户展示隐私政策的核心内容，并提醒用户阅读隐私政策。仍存在APP存在“默认勾选”同意或采取“注册即同意（隐私政策）”的方式，如高德地图、遇见Meet等。

今年国家网信办已通报地图导航、输入法、安全管理、短视频等多类头部应用，针对“七类”超范围收集行为进行了重点整治，包括超范围收集用户通讯录、精确地理位置、短信、通话记录等在内的一大批与人民群众切身利益相关的违法违规问题得到治理。

《个人信息保护法》进一步细化了“基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出”等要求。根据国家网信办等四部委发布的《APP违法违规收集使用个人信息行为认定方法》，目前常见违反知情同意要求的问题集中表现为以下四类：

征得用户同意前收集个人信息

监测发现，2万中小应用样本在同意隐私政策前将用户安卓ID等信息上传至云端服务器，4.4万中小应用样本没有向用户提供明确的隐私政策拒绝选项。

用户拒绝后频繁征求用户同意、干扰用户正常使用

13万存量中小应用样本在用户明确拒绝授权后，仍然在使用过程中频繁索取权限，或者用户下次进入应用再次索取权限；且人工抽验显示，在近三个月新上架应用中仍普遍存在频繁索权的问题。

诱导用户同意收集个人信息

例如，以签到、福利等为理由诱导用户提供姓名、手机号、住址，以“绝不收集隐私信息”等欺骗性提示诱导用户安装使用APP等。

○ 个人信息进行定向推送但无法关闭

有27万个应用样本声明会利用个人信息进行定向推送，但人工抽验发现，除了新闻资讯、网络直播、短视频等部分类别外，大多未提供关闭定向推送的选项。此外，部分APP尽管提供了关闭选项，但还存在为关闭选项强制设定了几个月的有效期，到期后自动恢复定向推送，关闭选项极其隐蔽，普通用户难以发现，关闭定向推送后并不生效等问题。

《“十四五”信息通信行业发展规划》报告指出，截至目前，工信部已组织检测21批次共244万款APP，累计通报2049款违规APP，下架540款拒不整改的APP，对违规行为持续保持高压震慑。同时，工信部不断强化应用商店关键责任链管理，督促应用商店加强自查清理，应用商店已主动下架40余万款违规APP。

同时，2021年工信部针对用户反映强烈的APP超范围、高频次索取权限，非服务场所必须收集用户个人信息，欺骗误导用户下载等违规行为进行了检查，共发现38款APP存在问题。

序号	应用名称	应用开发者	应用来源	应用版本	所涉问题
01	腾讯新闻	深圳市腾讯计算机系统有限公司	应用宝	6.6.51	欺骗误导强迫用户 应用分发平台上的APP信息明示不到位
02	全民K歌 极速版	腾讯音乐娱乐科技（深圳）有限公司	应用宝	7.7.28.278	强制用户使用定向推送功能 欺骗误导强迫用户
03	QQ音乐	深圳市腾讯计算机系统有限公司	应用宝	10.18.5.9	超范围收集个人信息
04	小红书	行吟信息科技（上海）有限公司	应用宝	7.13.0	超范围收集个人信息
05	探探	探探文化发展（北京）有限公司	应用宝	4.8.8.2	超范围收集个人信息
06	作业帮	小船出海教育科技（北京）有限公司	应用宝	13.25.2	超范围收集个人信息
07	看看新闻	看东方（上海）传媒有限公司	应用宝	6.1.7	超范围收集个人信息 APP强制、频繁、过度索取权限
08	我的日程表	有鲤科技（厦门）有限公司	应用宝	1.2.4	超范围收集个人信息
09	亚朵	上海亚朵商业管理（集团） 股份有限公司	360手机助手	3.13.0	违规收集个人信息 超范围收集个人信息 违规使用个人信息 强制用户使用定向推送功能 欺骗误导强迫用户
10	影视大全	襄阳品山信息科技有限公司	360手机助手	4.2.5	超范围收集个人信息 欺骗误导强迫用户 应用分发平台上的APP信息明示不到位
11	宝宝树孕育	宝宝树（北京）信息技术有限公司	vivo应用商店	8.60.0	超范围收集个人信息
12	妈妈网孕育	广州盛成妈妈网络科技股份有限公司	vivo应用商店	11.10.3	超范围收集个人信息
13	动动	北京百索科技有限公司	vivo应用商店	8.7.1.1	超范围收集个人信息
14	嗨呀星球	武汉佐趣科技有限公司	vivo应用商店	2.3.6	APP强制、频繁、过度索取权限
15	豆豆免费小说	北京友和卓谊信息技术有限公司	vivo应用商店	5.6.0	APP强制、频繁、过度索取权限 欺骗误导强迫用户
16	微商水印Pro	北京助梦工场科技有限公司	vivo应用商店	5.2.88	APP强制、频繁、过度索取权限

数据来源：工信部官网APP超范围索取权限、过度收集用户个人信息等问题通报

序号	应用名称	应用开发者	应用来源	应用版本	所涉问题
17	班级优化大师	广州视睿电子科技有限公司	vivo应用商店	3.0.33.1	APP强制、频繁、过度索取权限
18	搜狐资讯	北京搜狐新媒体信息技术有限公司	小米应用商店	5.3.12	APP强制、频繁、过度索取权限 欺骗误导强迫用户
19	爱回收	上海万物新生环保科技集团有限公司	小米应用商店	5.8.0	违规收集个人信息 超范围收集个人信息 违规使用个人信息 APP强制、频繁、过度索取权限
20	百合婚恋	百合佳缘网络集团股份有限公司	小米应用商店	11.3.0	超范围收集个人信息 欺骗误导强迫用户
21	VUEVlog	北京跃然纸上科技有限公司	小米应用商店	3.21.2	超范围收集个人信息
22	斗米	北京世纪优聘科技发展有限公司	小米应用商店	6.9.16	APP强制、频繁、过度索取权限
23	安心输入法	北京芯盾集团有限公司	小米应用商店	1.1.0.9	APP强制、频繁、过度索取权限
24	拍拍语音	爱语游网络科技（上海）有限公司	小米应用商店	1.14.0	APP强制、频繁、过度索取权限
25	UC浏览器 极速版	优视科技（中国）有限公司	豌豆荚	13.5.2.1114	欺骗误导强迫用户 应用分发平台上的APP信息明示不到位
26	58同城	北京五八信息技术有限公司	豌豆荚	10.22.4	超范围收集个人信息
27	货拉拉	广州依时货拉拉科技有限公司深圳分公司	豌豆荚	6.5.82	APP强制、频繁、过度索取权限
28	豆瓣	北京豆网科技有限公司	豌豆荚	7.16.0	超范围收集个人信息
29	唱吧	北京小唱科技有限公司	豌豆荚	10.8.2	超范围收集个人信息
30	乐教乐学	北京世纪飞育软件有限责任公司	豌豆荚	1.0.245	超范围收集个人信息
31	必要	珠海必要科技有限公司	豌豆荚	5.63.0	违规收集个人信息 APP强制、频繁、过度索取权限
32	平安金管家	中国平安人寿保险股份有限公司	华为应用市场	7.09.21	超范围收集个人信息
33	启信宝	上海生腾数据科技有限公司	华为应用市场	8.1.1.0	超范围收集个人信息
34	趣淘生活	成都优狸多多科技有限公司	华为应用市场	1.5.7	超范围收集个人信息 强制用户使用定向推送功能 APP强制、频繁、过度索取权限 应用分发平台上的APP信息明示不到位
35	有趣生活	杭州砍一砍网络科技有限公司	华为应用市场	1.3.3	违规收集个人信息 超范围收集个人信息 违规使用个人信息 强制用户使用定向推送功能
36	周末酒店	上海尚旅网络科技有限公司	OPPO软件商店	7.3.10	违规收集个人信息 违规使用个人信息 强制用户使用定向推送功能 APP强制、频繁、过度索取权限
37	刷宝	深圳市移卡科技有限公司	OPPO软件商店	3.4.5（001）	超范围收集个人信息 APP强制、频繁、过度索取权限
38	氧气语音	湖南大写信息科技有限公司	OPPO软件商店	9.16.3	APP强制、频繁、过度索取权限

数据来源：工信部官网APP超范围索取权限、过度收集用户个人信息等问题通报

2 由安全事件导致的个人信息泄露典型事件分析

大众遭黑客攻击，超300万奥迪车主个人信息被窃取

2021年3月，大众汽车集团美国公司发现，负责为其提供销售与营销服务的第三方供应商遭遇数据泄露事件。由于该供应商的某套在线系统存在配置错误，导致其被黑客攻击，致使超过330万客户的个人信息意外流出，其中大部分为奥迪车主。

大众汽车发现数据泄露问题后便及时通知供应商，但供应商未能及时解决，直到2个月后事件才得到彻底解决。此事件影响一部分特定大众客户，导致其敏感信息公开。

大众汽车表示，个人信息泄露的范围包括奥迪车主及潜在买家相关的联系方式与车辆信息，包括以下部分或全部联系信息：姓名、个人或企业收件地址、电子邮件地址或电话号码。部分客户泄露的数据还包括实际购买、租赁或查询的车辆信息，包括车辆识别号（VIN）、品牌、型号、年份、颜色及内饰选配包。

泄露的用户中，约9万名奥迪车主或潜在买家受到的影响最大，泄露信息包括购买、贷款或租赁资格等敏感内容。并且，超过95%都涉及驾照号码，甚至有极少数记录包含出生日期、社保或保险号码、账户或贷款号码以及税号等。

大众汽车表示，这批外泄的数据来自2014年至2019年期间的美国及加拿大客户。

在信息泄露后不久，一批据称从暴露AzureBLOB容器中窃取的奥迪与大众客户数据在外国一高人气黑客论坛上公开出售。在售数据包含超过500万条记录，其中386万2231条为导购记录、179万2278条来自销售数据库。导购数据库中包含潜在客户的联系信息与电话号码，而销售数据库中的数据则更为丰富，具体涵盖车辆识别号、商业编号、驾驶人信息以及车辆信息。

黑客们为全体记录开出了4000到5000美元的价码，并表示目前在售的数据库中不包含任何客户的社保号码。

同时，该黑客组织宣称，他们已经以1000美元的价格将数据库出售给某VPN服务商，这家服务商在GooglePlay商店中有多款应用在售。

魔蝎公司非法爬取个人信息两千万余条

爬虫是一种按照一定的规则，自动地抓取网络中信息的程序或者脚本。爬虫本身只是一种程序，比如，当你在搜索引擎中进行搜索时，实际上搜索的内容本身便是搜索引擎定时从各大网站中爬取的数据。爬虫也可被用于恶意活动中，比如人们所常见到的恶意抢票软件，就是以高频率在购票网站中爬取余票。像人们在登录过程中常见的输入验证码的机制，实际上就是在阻拦一些爬虫程序，然而，即便有了验证码等登录方式的阻拦，爬虫程序依然猖獗。对于购票软件，如12306，公开数据显示，其最高峰时一天内页面浏览量达813.4亿次，1小时最高点击量59.3亿次，平均每秒164.8万次。

魔蝎科技成立于2016年，是国内领先的大数据智能风控服务供应商，为2000多家银行、消费金融、保险、互联网金融等客户提供精准营销评分模型、反欺诈、多维度用户画像、授信评分、贷后预警、催收智能运筹等全面风险管理服务。

经查，魔蝎科技主要为网络贷款公司、银行提供用户个人信息及多维度信用数据，并从中收取服务费。魔蝎科技将开发的前端插件嵌入网贷平台APP中，网贷平台用户使用网贷平台的APP借款时，首先需要在魔蝎科技提供的前端插件上输入其通讯运营商、社保、公积金、淘宝、京东、学信网、征信中心等网站的账号、密码。

经过用户授权后，魔蝎科技的爬虫程序即代替用户进入其个人账户，利用各类爬虫技术，爬取上述企、事业单位网站中贷款用户本人账户内的通话记录、社保、公积金等各类数据，并按与用户的约定将数据提供至网贷平台用于判断用户的资信情况，并从网贷平台获取每笔0.1元至0.3元不等的费用。在此过程中，魔蝎科技存在欺骗用户的情况，并对用户信息进行永久保存。

根据魔蝎公司在和个人贷款用户签订的《数据采集服务协议》，魔蝎科技明确告知贷款用户“不会保存用户账号密码，仅在用户每次单独授权的情况下采集信息”，但在实际使用过程中未经用户许可，仍采用技术手段长期保存用户隐私信息并存于租用的阿里云服务器中。

截至2019年9月案发时，法院等部门对魔蝎公司租用的阿里云服务器进行勘验检查，发现以明文形式非法保存的个人贷款用户各类账号和密码条数多达2000万余条。

西湖法院认为，魔蝎科技以其他方法非法获取公民个人信息，情节特别严重，其行为已构成侵犯公民个人信息罪，判处罚金人民币三千万元；被告人周某某犯侵犯公民个人信息罪，判处有期徒刑三年，缓刑四年，并处罚金人民币50万元；被告人袁某犯侵犯公民个人信息罪，判处有期徒刑三年，缓刑三年，并处罚金人民币30万元。

英伟达公司1TB内部敏感数据失窃后遭勒索

国际芯片制造巨头英伟达证实，公司在2022年2月23日遭遇了一次网络攻击，入侵者成功访问到专有信息与员工登录数据。

2022年2月25日，一个名为Lapsus$的数据勒索团伙宣称袭击了英伟达内部网络，并在网上公开关于攻击事件的具体情况。

被入侵电子邮件警报网站HaveIBeenPwned表示，此次黑客攻击的范围包括惊人的71000名英伟达员工的电子邮件和密码哈希值，这些信息可以使黑客能够破解密码。黑客宣称他们已经掌握1TB大小的英伟达专有数据，包含40系显卡及后续产品计划、禁止挖矿限制、DLSS源代码，并公开了员工内网账号的密码哈希。

Lapsus$声称，英伟达曾通过尝试加密被盗数据反过来入侵黑客组织，但是Lapsus$已在虚拟机环境中制作了副本，这意味着反击措施没有成功。

攻击者使用虚拟机通过员工使用的VPN连接到英伟达内部网络，而英伟达要求用户必须在MDM（MobileDevice-Management）上进行登记才能连接VPN。攻击者认为英伟达通过反向追查发现了攻击者使用的虚拟机并进行了加密处理，并且切断了攻击者对英伟达内部网络的访问。

Lapsus$黑客组织提出了一个不同寻常的大众主义要求：他们希望英伟达永远开源其GPU驱动程序并删除其所有来自Nvidia30系列GPU的以太坊加密货币挖矿nerf，而没有直接勒索现金。该组织呼吁英伟达删除其有争议的禁止挖矿（LHR）功能。Lapsus$在Telegram上表示。「如果他们删除LHR，我们就会删除获取的内容，我们都知道LHR会影响采矿和游戏。」

但他们显然也想要现金。这些黑客公开表示，他们将以100万美元的价格出售加密nerf的bypass，随后，Lapsus$增加了另一个需求：它希望英伟达开源其用于macOS、Windows和Linux设备的图形芯片驱动程序。该组织要求英伟达在3月4日之前遵守，英伟达目前没有作出回应。

3 应用软件越权获取数据典型事件分析

猎豹清理大师APP违规索取通讯录权限

中国消费者协会发布的《APP个人信息泄露情况调查报告》显示，85.2%的受访者曾遭遇过个人信息泄露。其中，经营者未经授权收集个人信息和故意泄露信息是造成消费者个人信息泄露的主要途径。

2020年5月，“猎豹清理大师”APP因其隐私协议中对于索取用户通讯录、通话记录等权限的行为没有进行详细说明被国家工信部通报，北京市公安局朝阳分局已依法责令该公司改正违法行为。

猎豹清理大师是由金山网络开发的智能手机应用。它可以清理智能手机上的应用缓存、残余程序文件、历史痕迹以及应用程序安装包。该APP已在全球下载量超过十亿。然而，该APP在没有向用户说明的情况下，未经授权索取用户通讯录、通话记录等权限。

工信部通报后，猎豹清理大师声明：“猎豹清理大师从来没有、也绝对不会上传任何用户本地通讯录和通话记录信息”。

猎豹清理大师在V6.13.5之前的版本中曾经加入游戏《王者荣耀》的加速功能，该功能会在开启时会主动征询用户授权，请求用户授权通讯录权限和通话记录权限，以实现游戏免打扰和帮助用户回复游戏短信等功能。在2018年，猎豹清理大师已对该游戏加速功能进行了下线，但应用保留了部分代码，导致被检测出仍会调用上述两项权限，但并未上传任何信息。在接到公安部门的检测报告后，猎豹清理大师已在第一时间对产品进行了更新，移除了相关冗余代码。

如果说对猎豹清理大师这款APP来说，未经授权调用权限仅是由于工作失误，但在缺乏监管的情况下，对很多中小型APP而言，此类现象却是层出不穷。《100款APP个人信息收集与隐私政策测评报告》指出，其中被调查的APP普遍存在涉嫌过度收集个人信息的情况，其中有59款APP涉嫌过度收集“位置信息”，28款APP涉嫌过度收集“通讯录信息”，23款APP涉嫌过度收集“身份信息”，22款APP涉嫌过度收集“手机号码”等。

对于APP违规搜集个人信息的问题，光明日报与武汉大学法学院、网络治理研究院组成联合调研组，对1036人进行问卷调查及深度访谈。调查显示，各年龄段都有60%以上的用户遭遇垃圾短信与骚扰电话等威胁，部分APP过度索取数据调用权限，窃取地理定位、通讯录等本不应获取的信息，并私自提供给第三方，中下游再对此加工处理，致使个人信息流向不良商家。

在调查中，有25款APP的隐私协议包含很多与正当业务明显不相关的收集项。如地图导航类APP必须授权的信息中出现通讯录权限，受访者表示：“地图需要定位是很合理的，但是它不止一次向我索要通讯录的内容”。

在使用APP时，用户往往首先需要选择同意“使用协议”及“隐私协议”，然而目前存在这样的一个现象：用户不愿意阅读冗长的协议，而一旦选择拒绝，又面临着无法使用APP的局面。在这样的情况下，这种单一选择“同意”的情况成为毫无选择的形式之举。调查发现，否定选项不明显、点击“不同意”则强制退出等原因极大打击了用户认真阅读隐私协议的积极性。即使阅读后对协议内容有所质疑，也无法在“不同意”的基础上继续使用，这种毫无疑义的所谓“选择”成为人们放弃阅读隐私协议的主要推手。

超过一半的用户表示，使用的APP一旦同意隐私协议，便不允许撤销部分或者全部授权。调查的150款APP隐私协议文本仅有52.7%允许用户撤回同意，且只允许通过注销账户来实现撤回，但注销账户非常困难，甚至没有明确标注注销方式。调查中存在这样一种情况：何先生在注册某购物APP账号时使用了身份证号和手机号，因担心信息泄露所以申请注销账号并解除身份证绑定，但是APP客服要求其提供手持身份证照片进行审核，何先生觉得无法接受提供此类敏感信息，最终无法注销账号。

《移动互联网应用程序信息服务管理规定》第七条指出，移动互联网应用程序提供者应当严格落实信息安全管理责任，依法保障用户在安装或使用过程中的知情权和选择权，未向用户明示并经用户同意，不得开启收集地理位置、读取通讯录、使用摄像头、启用录音等功能，不得开启与服务无关的功能，不得捆绑安装无关应用程序。

《“十四五”信息通信行业发展规划》报告指出，截至目前，工信部已组织检测21批次共244万APP，累计通报2049款违规APP，下架540款拒不整改的APP，对违规行为持续保持高压震慑。同时，工信部不断强化应用商店关键责任链管理，督促应用商店加强自查清理，应用商店已主动下架40余万款违规APP。

随着相关政策的不断完善，《个人信息保护法》的实施，以及相关部门的大力监管督查，此类APP“乱象”有了更加明确的法律依据，目前已逐步得到治理。个人信息的防护，最终还是需要公民个人具有良好的隐私保护意识，APP存在的侵权问题最终还是要落于个人进行发现和检举。

4 数据滥用典型事件分析

携程APP“大数据杀熟”维权案

“杀熟”，简单理解就是，同样的商品或服务，新用户和老用户看见的价格不同，往往老用户会价格偏高。大数据“杀熟”指的便是通过大数据手段，例如用户画像，精准将用户定位，利用线上消费用户“天然隔离”的特点，使消费者无法及时有效识别价格的不同。网络购物、在线订票、外卖和网约车等互联网消费领域是大数据杀熟的“重灾区”。

当平台通过大数据手段获取了你的购买习惯，例如购物喜好，是否有比价习惯，常购买的价格区间等，就会逐步完善你的用户画像，标记你为价格不敏感的“粘性客户”，并按照你的购买习惯推荐商品，甚至修改商品的价格。假若你是新用户，平台为了用户留存，往往还会给予你一些价格上的优惠，再给出一段“养熟期”。

究其原因，大数据“杀熟”一方面是利益驱动使然。另一方面则源于平台在技术、信息等方面，对消费者拥有压倒性优势，用户只能被迫接受信息，往往面临着举证不易、维权困难的困境。此外，大数据“杀熟”的关键原因，即是在于平台对用户数据的保护和利用不当。

近几年来，存在这样的一个现象：当登录某个应用软件时，用户必须选择同意用户协议以及其获取权限的要求，否则便无法正常登录。用户为了使用软件，让渡了自己的部分数据权利。例如，让平台获取自己的消费习惯、消费能力、商品偏好、价格敏感等信息。然而，这并不意味着平台可以随意使用这些用户数据，或者利用信息不对称进行牟利。大数据“杀熟”严重侵害消费者权益，如果任由发展，不利于电商行业的持续健康发展。

《个人信息保护法》第十六条规定，个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外。

根据北京市消费者协会2019年3月发布的“大数据杀熟”问题调查结果，88.32%被调查者认为“大数据杀熟”现象普遍或很普遍，56.92%被调查者表示有过被“大数据杀熟”的经历。

有媒体报道，周女士准备带家人去海南度假，为节约路费，从一个月前就在携程开始关注机票价格，多次搜索后，机票价格却比最初价格贵了1000元，而朋友去预定相同的航班的价格却比自己低几百元。这就是一个典型的“大数据杀熟”的案例。

2021年7月7日，绍兴市柯桥区法院审理了胡女士诉上海携程商务有限公司侵权纠纷一案，该案是绍兴首例消费者在质疑遭遇“大数据杀熟”后成功维权的案例。

法院经审查表明，该案原告胡女士此前多次通过携程APP预订机票、酒店，在携程平台上消费了10余万元，成为该平台的钻石贵宾客户。去年，胡女士像往常一样通过携程APP订购了舟山某高端酒店的一间豪华湖景大床房，支付价款2889元。但胡女士在退房时，发现酒店的挂牌房价加上税金总价仅1377.63元。“不仅没有享受到星级客户应当享受的优惠，反而多支付了一倍的房价。”胡女士随后与携程反映情况。携程以其系平台方，并非涉案订单的合同相对方等为由，仅退还了部分差价。

胡女士以上海携程商务有限公司采集其个人非必要信息，进行“大数据杀熟”等为由诉至法院，要求退一赔三并要求携程APP为其增加不同意“服务协议”和“隐私政策”时仍可继续使用的选项，以避免被告采集其个人信息，掌握原告数据。

柯桥区法院审理后认为，携程APP作为中介平台对标的实际价值有如实报告义务，其未如实报告。携程向原告承诺钻石贵宾享有优惠价，却无价格监管措施，向原告展现了一个溢价100%的失实价格，未践行承诺。并且，携程在处理原告投诉时告知原告无法退全部差价的理由，经调查也与事实不符，存在欺骗行为。故认定被告存在虚假宣传、价格欺诈和欺骗行为，支持原告退一赔三。

根据报文，新下载携程APP后，用户必须点击同意携程“服务协议”“隐私政策”方能使用，如不同意，将直接退出携程APP，是以拒绝提供服务形成对用户的强制。

而且，携程APP的“服务协议”“隐私政策”均要求用户特别授权携程及其关联公司、业务合作伙伴共享用户的注册信息、交易、支付数据，并允许携程及其关联公司、业务合作伙伴对用户信息进行数据分析，且对分析结果进一步商业利用。

携程APP的“隐私政策”还要求用户授权携程自动收集用户的个人信息，包括日志信息、设备信息、软件信息、位置信息，要求用户许可其使用用户信息进行营销活动、形成个性化推荐，同时要求用户同意携程将用户的订单数据进行分析，从而形成用户画像，以便携程能够了解用户偏好。

上述信息超越了形成订单必需的要素信息，属于非必要信息的采集和使用，其中用户信息分享给被告可随意界定的关联公司、业务合作伙伴进行进一步商业利用更是既无必要性，又无限加重用户个人信息使用风险。

招聘网站缺少限制，肆意售卖求职者简历

《个人信息保护法》第九条规定，个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。

作为收集、使用个人简历的招聘网站，需要对收集到的个人信息负行政责任，保护其个人信息安全。人力资源和社会保障部数据显示，截至2019年末，全国共有3.96万家人力资源服务机构，人力资源市场网站1.5万个，2019年发布网络招聘信息4.04亿条。网络招聘在为求职者提供快捷便利服务的同时，也出现了部分求职者投递简历后屡遭陌生来电和短信骚扰，甚至陷入非法传销、情色招聘陷阱等现象。其中很重要的一个原因，就是随着互联网的高速发展，倒卖公民个人信息往往能获得较大非法利益，一些不法分子为此铤而走险。

2021年3月15日晚，央视“3.15”晚会点名曝光了智联招聘、猎聘网求职者简历被售卖问题。

据中央广播电视总台报道，只要在智联招聘上注册企业账号，就可以很容易大量下载这些简历，但想要得到求职者姓名、电话、邮箱地址等关键信息，还会根据求职者的学历、工作经验、薪资水平等条件，支付40元、60元、100元三个等级不同的金额。

智联招聘还表示，只要肯花钱，企业用户就可以毫无限制地下载求职者的个人简历，求职者并不知道自己的简历被谁下载，拿去做了什么。

同样的事情还发生在猎聘网和前程无忧两个网络招聘平台。此外，在各类贴吧、论坛、QQ群里发现，出售招聘平台简历的信息也比比皆是。在一个名叫“58智联粉”的QQ群里，只需支付7元，便可买到一份智联招聘平台上的求职者简历，求职者的个人信息一应俱全。企业账户只要交钱办理会员，就可以不受数量限制下载求职者的完整简历，而在注册企业账户时，即使是伪造的资质申请也可以顺利通过。

凭借上述手段下载、购买简历后，不法分子能够获知公民的详细个人信息，从而实施精准诈骗。近年来，用户隐私信息被泄露倒卖，在互联网行业已不是少数个案，仅被警方公布的案例就不时见诸媒体，如某地警方破获的相关案件中，一名嫌疑人在硬盘中存储了700多万份求职者简历；2019年，智联招聘员工参与倒卖用户简历获刑，涉案简历多达16万份。

2016年10月至2018年6月，被告人黄某通过猜配密码的方式非法获取智联招聘企业客户账号，盗窃求职者简历并出售给被告人解某，获取违法所得人民币33万余元。被告人解某将从被告人黄某处非法购买的求职者简历加价转卖给被告人郑某，获取违法所得人民币27万余元。后郑某通过在淘宝网等网络平台开设的店铺非法对外出售。

此外，2018年3月至6月间，被告人郑某分别与智联招聘职员王某、卢某合谋，通过在智联招聘网站上开立虚假的企业账号等方式，非法获取求职者简历并用于出售。其中，卢某涉非法获取求职者简历并出售给郑某达12万余条，王某涉非法获取求职者简历并出售给被告人郑某4万余条，获取违法所得人民币33329元。

案卷显示，最终所有非法获取的信息都落入了郑某手中。郑某供述，他以3-5元/份的价格购入求职者简历，然后以5-8元的价格在淘宝售出，支付宝收款。简历内容包括详细的公民个人信息，如求职者名字、出生年月、年龄、性别、工种、职业、职务、学历、受教育经历、岗位经验、手机号码、电子邮箱、求职意向等。大概卖了几十万份，流水300万元左右，盈利约150万元。

这起智联招聘员工参与倒卖公民个人信息案于2019年8月30日在北京朝阳法院一审公开宣判。该案涉及公民个人信息达16万余份。郑某及智联招聘员工等5人分别因侵犯公民个人信息罪被判处有期徒刑4年至4年九个月不等的刑罚，并处罚金5万至30万元。

2021年3月17日，北京市人力资源和社会保障局针对央视3·15晚会点名曝光的数据安全问题约谈了智联招聘、猎聘网两家涉事企业，要求智联招聘和猎聘网立即彻查彻改，严格落实《网络招聘服务管理规定》等法律法规，阻断不法分子倒卖求职者简历信息“利益链”，切实保护求职者合法权益。

市人力资源社会保障局表示，下一步将采取有力措施，进一步加强网络招聘行业监管。包括开展专项检查，严厉查处网络招聘服务中的各类违法违规行为，加大曝光和处置力度；完善制度体系，出台实施人力资源市场政府规章，进一步细化完善求职者个人信息保护有关要求；加强行业自律，督促网络招聘企业严格履行求职者信息保护主体责任，营造更安全的求职招聘环境。

个人信息与隐私保护挑战典型场景

人工智能应用

人工智能具有巨大的社会价值，但也会提出一系列的法律挑战。其中，人工智能引发的隐私保护问题尤为显著，已经成为当前最具挑战性的话题。在人工智能时代，我们每个人都生活在数据与算法之中，人工智能的核心技术是数据与算法，这意味着人工智能越智能，就越需要海量的个人信息作为支撑，同时也意味着处理个人信息的能力也就越强，由此引发严重的隐私安全危机。人工智能具有超强的“画像识别”能力。借助物联网、大数据等技术，人工智能的数据整合和分析能力得到极大地增强，能够轻易地描绘出用户的完整“画像”。人工智能时代的隐私保护困境主要集中体现为如何处理好个人信息利用与隐私保护之间的关系。“刺猬困境”形象地描述了个人信息使用与隐私保护之间的辩证关系。

元宇宙隐私安全

元宇宙（Metaverse）是利用科技手段进行链接与创造的，与现实世界映射和交互的虚拟世界，具备新型社会体系的数字生活空间。自2021年以来，元宇宙热度在全球范围内持续上升，国内元宇宙市场火爆。据摩根士丹利近期发布的简报预测，中国“元宇宙”市场的潜在总规模将高达52万亿元人民币（约8万亿美元）。元宇宙不仅是下一代互联网，更是下一代数字经济。从社会、经济、文化三大角度出发，元宇宙会为社会信用体系、价值交换、生产关系等种种既定规则带来改变，同时将衍生出多类场景，解决当前移动互联网时代存在的诸多问题。

然而，元宇宙的火热引发了隐私安全危机，元宇宙将现实生活与虚拟和增强世界紧密联系在一起。在元宇宙中，用户看到的增强世界将在每个人之间共享。这意味着可以轻松共享数据，可以与任何连接的用户交互，并且用户可以立即获取其他用户的信息。因此，元宇宙意味着在每个人的工作和生活场景中将会有更多更智能的环境感知和信息收集终端。

元宇宙收集的个人数据的数量和丰富程度将是前所未有的，包括个人生理反应、运动，甚至可能是脑电波数据。这些数据是否会聘请专门的安全公司来负责其数据安全性？如果用户的个人数据在元宇宙中被盗或滥用，谁来负责，会对现实世界的用户产生什么影响等。在元宇宙的建设当中，需要严格考虑此类个人信息的隐私问题以及设置良好的机制来防止个人隐私信息的外泄。

生物识别技术

生物识别技术是一类基于个体独特的生理或行为特征对个体身份进行自动辨识或认证的技术。主要包括指纹识别、人脸识别和虹膜识别等技术。相比传统的密码形式的识别方式，生物识别具有更加准确、方便快捷和不易遗忘等优点。目前人们对身份认证的要求越来越严格，传统的识别方式已经不能满足人们对于更高安全等级的需要，新兴的智能生物识别技术正是在这种社会背景下迅速发展起来。早在2008年，我国研制的人脸识别技术成功用于北京奥运会；2013年，苹果公司推出指纹手机；2015年，生物识别技术开始入驻我国社保卡领域；2015年3月，全国首家人脸识别医保支付系统在武汉市中心医院上线；2016年底，北京西站启用人脸识别系统，旅客可刷脸进站；2017年，澳大利亚当地移民及边境保护局计划于机场设立电子扫描站，利用生物识别技术辨认入境游客的面孔、眼睛虹膜及指纹。可以说，随着计算机技术的不断发展、成本的持续降低以及性能的稳步提高，生物识别技术变得更加具有实用性，应用范围也更加广泛。

然而，在生物识别技术取得广泛社会应用给人们带来巨大收益的同时，也带来了对隐私保护问题的担忧。

生物识别信息与其他个人信息不同，其一旦泄露或被盗，将很难或不能重新设置。如一个指纹信息被盗，可以换别的手指，但这样的更换最多也就9次。而一旦面部特征被盗，除非换脸或使用传统的识别方式，没有其他很好地补救办法。因此，生物识别信息的永久性带来的影响将会是深远的、不可逆的。

生物识别信息跟密码、口令之类的个人信息不同，指纹和面部特征都在人体的表面，很容易被窃取：仅仅在物体的表面按压，就可以留下个人的指纹信息；仅仅通过面部的高清照片，就可以获得个人的面部特征。加之目前互联网技术的开放发展、高清图像处理技术的提升以及3D打印等技术的不断进步，个体很难知道什么人在哪些情况下可以获取他们的生物识别信息以及使用这些信息的目的是什么，因而个体也几乎意识不到他们的隐私可能正在被侵犯。

无人驾驶汽车

无人驾驶汽车是一种智能汽车，主要依靠车内的以计算机系统为主的智能驾驶来实现无人驾驶。无人驾驶汽车集自动控制、体系结构、人工智能、视觉计算等众多技术集于一体，作为人工智能的典型应用，无人驾驶的价值功能显著而广泛，包括但不限于如下方面：一是减少交通事故发生；二是缓解交通拥堵；三是增加特定人群的行动自由。

无人驾驶技术犹如一枚具有正反两面的硬币，亦是一把双刃剑，在为人类服务的同时，也附带了一系列安全风险。无人驾驶汽车在广泛应用中可能会收集的个人隐私信息主要包括：姓名、肖像、声音、住址、通信信息；二是乘客在车内的个人活动，包括但不限于亲密行为、言谈举止、聊天记录，有时还会涉及工作事务，可能会被录音、录像；三是自然人不愿意公开的出行轨迹；四是乘客的财产类信息，如交易记录、支付账号等；五是驾驶员或其他乘客的健康类数据。

一旦这些隐私数据被智能系统记录且经过加工利用，生产者或互联网企业从中获取利益，就会构成对个人隐私的侵犯。因此这里面临两个问题。一是汽车制造商获取上述个人信息的正当性和必要性，以及如何采集、传输、存储、使用、分享以及销毁汽车用户的个人信息，并对可能的隐私侵权风险提供何种安全保障措施；二是如何保障无人驾驶汽车控制系统和车联网通讯系统的安全性，防止系统被入侵或个人隐私信息泄漏。

可穿戴设备

智能可穿戴设备主要分为消费级智能可穿戴设备和医用级智能可穿戴设备，其中，消费级智能可穿戴设备主要针对普通健身爱好者，通过对运动量、心率、呼吸睡眠、热量消耗、体脂测量等健康指征进行监测实现自我健康管理；医用级智能可穿戴设备主要服务对象为各类疾病患者人群：一是监测功能，是指对特定疾病患者人群进行体温、血压、血糖、供氧、心电等体征数据进行实时监测，确保患者各项健康指标在正常范围值内，实现患者健康风险防范；二是治疗功能，是指对一些慢性病患者人群进行指导管理、干预治疗等。

但是可穿戴设备通常使用无线传输进行敏感信息的传输，在敏感数据传输中易被非法获取，进而获取用户敏感信息。同时可穿戴设备更注重功能开发而本体安全相对较为薄弱，对于攻击行为表现得比较滞后，美国前副总统Dick Cheney就因担心恐怖分子会入侵他体内植入的医用心脏除颤器实施致命电击，而关闭了除颤器的无线管理功能。

健康医疗领域

医疗行业的信息技术应用水平飞速发展得到显著提升，互联网医疗、医疗数据应用等新业务不断涌现，由于医疗数据安全关于患者生命安全、个人隐私保护、社会公益，乃至国家安全，医疗数据在全生命周期各个阶段都面临着极大的安全挑战。

其一，互联互通大趋势导致数据暴露面增加：医院在互联互通、高等级电子病历、互联网医院的建设过程中，不可避免地促使数据在不同系统、不同院区甚至不同医院间流转，也会面对来自互联网甚至物联网的数据访问请求。数据通道数量的增加导致数据安全出现问题的概率也在成倍增加。

其二，数据复杂度增加导致治理困难：医院信息系统产生的数据日益复杂，从最早的电子病历与HIS数据，到现在PACS、LIS、甚至物联网都在时刻产生着庞大数据。各种数据格式不一、内容庞杂，缺乏安全分级分类标准，无法定义安全保护等级，导致治理困难，从而使安全策略难以细粒度实施。

其三，数据防护思路手段落后无法应对挑战：传统基于数据库审计与访问控制的数据安全体系无法应对目前的数据使用场景，例如医院数据向外部交换时的安全防护、拟人化木马数据窃取、账号失窃后的数据访问等；

其四，外部攻击挑战：医疗过程中产生的诊疗、健康数据在临床辅助诊疗和健康管理方面具有极高的价值，是企业和国际竞争中引人注目的新的技术焦点；

同时，诊疗期间涉及的支付数据、个人隐私数据等信息，也对很多黑灰产业者具有极高的吸引力。此外，勒索攻击者普遍认为，医疗数据作为涉及人身安全和个人最隐私的信息，倘若因勒索病毒感染导致数据丢失、业务系统中断，就会将患者的生命置于风险之中，且会面临上级部门的问责，因此从业者往往会不惜代价马上支付赎金解锁数据，而不是苦等数据从备份中恢复出来。这些都是导致医疗数据极易引发外界攻击的主要原因。

在2020年12月14日，国家市场监督管理总局与国家标准化管理委员会正式发布了国标《信息安全技术健康医疗数据安全指南》（GB/T39725-2020），自2021年7月1日起实施。该安全指南明确定义了健康医疗数据，并制定了健康医疗数据分类体系、使用披露原则、安全措施要点、安全管理指南、安全技术指南及典型场景。进一步指明了健康医疗机构在保护个人信息以及个人健康隐私信息的安全防护路径。

电子商务及物流领域

据统计局、中商产业研究院数据显示，中国电子商务交易额从2016年的26.1万亿元增长至2020年的37.21万亿元，年复合增长率9.27%，2021年年底将达到40万亿元。据国家邮政局发布数据，2021年全年，我国快递业务量达1083亿件，同比增长29.9%，人均77件。

在电子商务持续高速增长的背后隐藏着一群盯上个人信息的不法分子。一是部分经营者过度索取消费者的个人信息，比如手机APP下载安装过度索权、必须扫码注册等；二是经营者未经同意滥用消费者个人信息，比如将消费者购买产品的情况用作宣传、营销短信轰炸、大数据杀熟等；三是倒卖个人信息，如商家将消费者信息进行传播售卖，电信诈骗人员利用这些信息进行精准诈骗或者洗钱再进行转卖，信息泄露链条长，危害大；四是违法犯罪分子盗取消费者网购消费信息，冒充客服对消费者进行诈骗。

综合提升建议

1 个人层面

保护个人信息安全，不能仅仅依靠建立和完善法律法规、加强行业自律以及完善企业内部的规章制度，更需要提高个人信息的保护意识和在日常生活中注重隐私保护，从根源上保护自己的信息安全。

建立隐私保护意识

一是知晓隐私泄露危害

个人信息和隐私信息的泄露，被不法分子利用后会给自己带来非常多的危害。垃圾短信、骚扰电话源源不断，已经是非常普遍的事情了，甚至被冒名办理信用卡恶意透支消费，造成巨大的财产损失，或者用来进行电信诈骗、洗钱，还会面临刑事法律风险。疫情防控期间多次个人信息的泄露事件还会使个人名誉受损。总之，个人信息和隐私的泄露不仅会给生活带来骚扰，还会影响财产安全、名誉受损、人身安全。大量的个人信息泄露被汇聚还可能危害社会甚至国家的安全。

二是强化隐私保护意识

- 要养成良好的上网习惯，对于来源不明的网站不要浏览、使用；
- 在使用移动应用时谨慎授予应用权限；
- 在网络上提交账号信息时，不填写过多的个人信息，例如真实姓名、电话号码、住址等，如确需填写，可做一定的技术处理，或者设置一定的访问权限；
- 需要删除的个人敏感文件应该进行粉碎处理，防止他人利用删除恢复软件进行恢复；
- 不在公共电脑上登录邮箱、即时通讯软件等，避免因留下登录信息而存在被盗号的风险；
- 不将个人照片、电话本等隐私信息上传到网盘、云盘等公共存储空间，避免由于这些公共存储空间本身的安全性和隐私性不强而造成泄露；
- 存储在U盘等移动存储设备上的重要或隐私文件要进行加密处理和防拷贝处理，防止丢失；
- 不在公共场所随意连接Wi-Fi，防止被网络钓鱼。

三是提升法律维权观念

在明确自身遭遇个人信息泄露并面临侵害时，相当一部分人群抱有侥幸心态，大部分人选择了较为被动的处理方式，仅有少部分人采取了积极对抗行动。这种侥幸心理不但使自身权益难以保障，也助长了不法分子的嚣张气焰。法律并不是一纸空文，更不是高高在上的，我们敬畏它的同时更应去尊法学法守法用法。国家法治社会的建设需要我们每一个人参与，自身利益更要我们义不容辞地去捍卫。我们应该学会增强自身法律观念，以此来维护自身权益，助己也助他。

个人日常生活隐私保护维护建议

对于个人用户，维护隐私保护的关键是“提高认识，注重细节”。在日常生活中，实体生活和网络活动中都存在泄露隐私信息，再通过网络和通信技术造成危害的可能。

在日常生活中，我们建议：

- 非必要情况下，不要随意登记自己的真实姓名、联系方式和身份证号码、银行卡号码等信息；
- 妥善保管自己的重要证件和银行卡片，尽量使用电子证照，丢失时尽快补办；
- 留存自己的身份证、银行卡和重要财产证明时，用马赛克隐去部分隐私或表明“XXX事项”专用水印；
- 不随意参加小调查、街头问卷、抽奖或免费赠送、非正规办卡等活动，不随意填写个人信息。不要轻信各种线下的营销、推广互动，向他人随意透露自己的隐私信息；
- 收集整理好含个人信息的票据，如快递单、车票、刷卡凭证等，集中销毁；
- 识别非法金融活动、传销行为，避免参与；
- 在遭到侵犯隐私的电话骚扰或其他犯罪侵害时，及时报警。

在上网用网时，我们建议：

- 安装全民反诈APP，根据提示，避免上当；
- 在公开网站平台填写信息时，避免用真名或拼写，非必要时不要在线填表，联系方式用截图方式，尽量用邮箱代替手机号码；
- 安装软件时一定要仔细阅读涉及个人隐私内容（如通讯录、短信等）的权限获取申请；
- 在不必要的情况下记得关闭软件定位，以免泄露个人位置信息；
- 不要在社交媒体随意公开自己及家人隐私信息；
- 及时注销、解除绑定长时间不使用的账户；
- 避免浏览不知名的网站、不随意下载来历不明的应用软件，不扫描陌生二维码；
- 不要浏览涉黄、涉毒、涉毒等非法网站，更不要在其引导下放开任何系统权限或下载软件；
- 及时关闭手机WiFi功能，在公共场所不要随便使用免费WiFi；
- 个人信息一旦被泄露，可向互联网管理部门和相关机构进行投诉举报。

2 企业层面

“能力越大，责任越大”。作为用户个人信息最直接的收集者、利用者和保护者，企业应该充分理解面临隐私合规监管环境、参考标准，联合制定企业的隐私保护合规制度。同时企业需要对自身的隐私保护成熟度和隐私数据现状进行识别。由于“个人信息的分布难以捉摸”，隐私数据现状识别工作会决定未来整体隐私保护工作落地的质量和有效性。

企业在进行隐私保护相关工作时应该特别注意以下几点：

- 一是企业应该识别明确在不同的业务模块、产品服务过程和数据活动中的角色，例如数据提供者、数据所有者、数据处理者、数据活动合作伙伴等。明确各方隐私保护义务和责任，为后续隐私保护管控制定特定化方案。
- 二是企业应对掌握的个人信息进行梳理，需要尽可能全面，注意识别个人信息的类型与敏感程度、个人信息全生命周期的情况以及已有的安全保护措施，并且需要特别考虑涉及的与第三方数据交互和共享场景下的相互保护义务和边界。
- 三是企业应对个人信息的处理活动进行梳理，识别个人信息动态风险，需要了解业务场景、产品服务、系统模块中个人信息处理的目的是什么，处理的主体是谁，个人信息流转的路径是什么，面临的风险是什么。
- 四是规划设计长效维护的梳理机制，确保隐私保护工作的持续有效性。
- 五是企业要积极响应参与国家以及行业协会隐私保护法律法规标准的制定，在遵守隐私合规义务的同时向上反馈新业态、新模式、新技术等场景下隐私合规面临的困境和风险。

企业在进行隐私保护防护体系建设时可选择采用以下技术：

- 一是零信任访问架构

  随着云、大、物、移等技术的快速发展和广泛应用，万物互联时代网络边界已经变得越来越模糊，传统以网络边界为核心的纵深防御体系的适用性以及面对新型攻击手段都表现得不尽如人意。已经无法适应5G、云计算、物联网等发展需求。零信任访问架构的核心是将传统以网络为基础的信任，变为以身份为信任的机制，关注针对数据、应用的动态访问授权和细粒度控制，建立先认证再连接的访问机制，能够快速提升信息系统的安全性，加强保障企业内部数据资源的访问控制，有效降低数据泄露与非法访问风险。因此零信任访问框架的应用对于数据资产保护，尤其是在新型互联网业态下的数据保护具有天然的优势，是保护企业数据资产、个人信息的坚固盾牌。

- 二是差分隐私技术

  种差分隐私保护模型（Differential　Privacy），主要用在数据发布和分析阶段带来的个人隐私泄露问题的解决方案。差分隐私保护具有严格、可量化的隐私保护机制，其保护强度不依赖以攻击者掌握知识多少，是在数据分析过程中随机添加噪声进而干扰攻击者达到保护隐私的目的。即使在数据库中删除或增加一个记录也不影响数据分析结果，攻击者获得除了一个特定的目标信息之外的所有内容也不能锁定和判断出这个记录内容。因此，很大程度上避免数据在发布、使用阶段隐私泄露的发生。差分隐私保护近年来是使用最多效果最好的技术，非常适用于交互环境下大数据分析、挖掘、信息发布等诸多领域。

三是数据加密技术

数据加密技术是传统的个人信息保护的方法，在大数据环境下它仍然是计算机系统中保护个人隐私主流技术，数据加密的主要功能是防止入侵者篡改、盗取数据。数据加密算法包含对称加密算法和非对称加密算法，所谓对称加密算法是指加密和解密是使用同一个密钥。这种加密算法只适合少量数据加密，不需要太大开销，随着数据量增长，数据分布式存储，很难保证密钥的安全性，并且成本开销较大；非对称加密算法是指加密和解密使用不同的密钥，主要应用在身份验证、数字签名等环节上，非对称加密算法使用与分布式网络环境中，虽然密钥管理容易，但算法较为复杂。

四是匿名化技术

匿名化方法是在数据发布之前将个人隐私数据掩藏起来，也是目前使用最多的个人隐私保护技术，应用最早的是K-Anonymity方法来保护个人数据隐私。匿名化方法可以根据不同类型攻击对个人数据进行保护，但缺点是当攻击者掌握碎片信息比较多时，通过结合发布的信息关联分析，就可能推断出某个人的属性信息，所以匿名化技术应该在方法上就进一步改进，适应不同格式或标识属性信息发布安全需求。

隐私保护技术还有同态加密、多方安全计算、区块链、联邦学习等等，安全技术的应用还要结合业务场景进行灵活选择。

3 行业协会层面

各行业协会（组织）积极颁布隐私保护指南以及行业标准，如行业数据分类分级指南等，指导企业的隐私保护实践。虽然指南和标准对企业不具有法律约束力，但是给行业发展确立了一个标杆和方向。为了获得更大的竞争优势，行业内的龙头企业会积极根据指南修改公司政策，起示范带头作用，逐渐带动行业内其他企业的参与，最终形成行业标准。

4 国家层面

建立健全法律法规

虽然当前已经发布《数据安全法》《个人信息保护法》等法律法规，从宏观层面上对数据权属、安全责任等进行了约束，但还需要加速出台可操作性更强的法律细则。当前公民个人信息安全意识强，但维权动力与能力有限，因此在法律条例中主要关注以下几方面个人权利和义务，首先，明确告知义务，企业或组织在收集个人信息时要明确告知信息提供者知情权、控制权。其次，明确使用方式和目的，信息收集者、使用者应该对收集到的个人数据使用目的、存储地点、适用范围以及期限进行详细规定，按政策要求个人信息提供者有权删除、修改，不允许过度收集。再次，注重隐私权，即不得随意拍摄、录制、泄露、跟踪他人的私人活动，不征求本人的同意而擅自公开、获取、买卖私人信息，如个人隐私受到侵害而采取相应的法律措施予以制止。

加强监管处罚力度

针对个人信息的非法获取与利用的司法判决为数不少，但与个人信息泄露的普遍状况相比，依然很少并不成比例。由于个人信息获取、存储和利用的环节众多，线下和线上传播具有隐蔽性和复杂性，追本溯源成本很高，发现、查处难度大，处罚、赔偿力度小，同时获利空间巨大，执法现状为灰色产业链提供了巨大的投机空间。特别是个人信息泄露与电信诈骗等犯罪活动结合之后，造成了重大的损失和巨大的社会影响，亟需加大惩处力度，增加犯罪成本，以切实起到威慑作用。对于造成精神损害的要追究责任和经济赔偿，对于造成受害人财产损失的除了承担民事责任外，情节严重的、危害较大的行为应纳入到刑事犯罪的范畴处理。加强政府监管，建立一整套安全评估体系，在法律框架下实施安全评价制度，引领企业、个人加强对隐私信息收集与管理。加大对泄露个人的问责机制和处罚力度，应用先进管理方法和法律法规来约束企业或组织的不法行为。

开展深度普法教育

国家层面上可以在媒体中推广个人隐私的保护方式，要加强信息安全意识的宣传，发放个人信息安全方面的文献并深入贯彻执行，定期举办科普讲座，利用一些网络平台发布公民信息安全知识。政府应将个人信息保护纳入国家战略资源的保护和规范范畴。