CAICT 中国信通院

电信和互联网用户个人信息保护白皮书

（2018 年）

CAICT 中国信通院

中国信息通信研究院

2018年11月

版权声明

本白皮书版权属于中国信息通信研究院，并受法律保护。转载、摘编或利用其它方式使用本白皮书文字或者观点的，应注明“来源：中国信息通信研究院”。违反上述声明者，本院将追究其相关法律责任。

CAICT 中国信通院

前　言

数字经济时代，大数据、人工智能等技术创新及广泛应用，个人信息的数据资源价值凸显，用户个人信息保护已成为用户权益保护的最主要、最热点领域之一。党的十九大报告提出“新时代中国特色社会主义思想，必须坚持以人民为中心的发展思想”，电信和互联网行业坚持这一基本思想，将用户利益摆在核心位置，高度重视用户个人信息保护工作。

近年来，全球范围内掀起了个人信息保护立法的浪潮，美国、欧盟、日本等先后制定或修订个人信息保护相关规定，确立了个人信息收集和使用的基本规则，逐步完善了个人信息保护制度。我国采取政府主导的监管模式，法规标准、企业自律、用户监督等方面多管齐下，推动个人信息保护水平提升。

随着个人信息链条延长，侵犯个人信息行为纷繁涌现，用户个人信息保护面临严峻态势，主要体现在感知层面智能设备的普及和多样化放大了个人信息收集的安全风险；网络层面数据传输量巨大，传输安全存在隐患；应用层面新技术的涌现挑战个人信息流通安全；商业层面企业收集使用个人信息存在泄露风险。如何在保护用户个人信息安全的同时努力做到合理、正当使用，成为了工作重点。

展望未来，持续开展用户个人信息保护工作，要平衡好个人信息安全和行业发展的双重需求，充分提高思想认识、把握关键原则、多种路径完善治理、探索新型技术应用，调动各方积极性，建立健全开放、协作、高效的多方参与的综合保护体系。

目 录

一、用户个人信息保护的内涵

（一）个人信息的概念分析

当前各国对个人信息的描述主要有个人信息、个人数据、个人隐私三类说法。日本、韩国等国家主要使用“个人信息”这一说法；美国、加拿大、澳大利亚等英美法系国家主要采用“个人隐私”这一概念；欧盟及其成员国习惯采用“个人数据”的称谓。本白皮书对这三种概念不做刻意区分。

全球对用户个人信息并无统一界定，可以是用来识别或反映特定个体的信息，如姓名、年龄、性别等；也可以是反映个体身份或行为有关的一套符号系统，如通信记录、信用历史等；还可以是与其他信息结合后能够识别到特定个体及其行为的信息。从立法态势而言，全球立法对个人信息的定义呈现趋同性，一切与个人身份及行为有关的内容都相继纳入个人信息的范畴。例如，欧盟《一般数据保护条例》（简称 GDPR）的定义是“任何指向一个已识别或可识别的自然人（数据主体）的信息；该可识别的自然人能够被直接或间接地识别，尤其是通过参照诸如姓名、身份证号码、定位数据、在线身份识别这类标识，或者是通过参照针对该自然人一个或多个如物理、生理、遗传、心理、经济、文化或社会身份的要素”。美国加州《消费者隐私保护法》（简称 CCPA）的定义则包括“直接或间接地识别、关系到、描述、能够相关联或可合理地连结到特定消费者或家庭的信息”，将生

物信息、教育信息等纳入其中。

国内立法使用的是“个人信息”这一术语。《网络安全法》的定义是“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”；《电信和互联网用户个人信息保护规定》的定义是“电信业务经营者和互联网信息服务提供者在提供服务的过程中收集的用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码等能够单独或者与其他信息结合识别用户的信息以及用户使用服务的时间、地点等信息”；《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》的定义是“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”。

此外，2018 年正式实施的国家标准《信息安全技术 个人信息安全规范》（GB/T 35273-2017）以资料附录的形式给出了个人信息和个人敏感信息的具体范围与类型，前者包括个人基本资料、个人身份信息、个人生物识别信息等；后者涵盖个人财产信息、健康生理信息等。

总的来看，用户个人信息的内涵基本稳定、外延愈发多元，伴随着技术的演进而不断扩展。

（二）个人信息保护的内涵演变

一些研究将全球的用户个人信息保护分为欧盟与美国两大模式，前者将个人信息视作基本人权加以保护，特点是重保护、轻应用；后者则建立在隐私权的基础上，通过保护公民隐私权来实现安全保护与行业发展之间的有效平衡。尽管欧盟与美国在用户个人信息保护方面采用了不同的立法模式和监管手段，但这种差异不能抹杀双方在该领域日益接近的事实，其实质是用户个人信息保护理念的全球共识正逐步形成。

早期的个人信息保护更多是纯粹的隐私权保护，哈佛大学的路易斯·D·布兰蒂斯和萨缪尔·D·沃伦在《哈佛法学评论》中将隐私权界定为“独处的不受干扰”的权利。随着经济社会发展及信息技术变革应用，个人信息既具有了人格权也具有了财产权的属性，既要安全可控也要合理使用。个人信息保护的内涵也逐渐发生变化。

上个世纪 70 年代初，美国提出了《公平信息实践法则》（简称 FIPPs），所包括的透明度、个人参与、目的明确、使用限制等成为个人信息保护制度的基石。随后，经济发展与合作组织（简称 OECD）在 1980 年发布《保护隐私和个人数据跨境流动指导原则》（简称 OECD 指南），其中提出的八项基本原则成为许多国家立法的依据。进入 21 世纪后，亚太经合组织借鉴了上述两份文件，制定了《APEC 隐私框架》，包括通知、收集限制、用户选择、确保个人信息完整性及采取必要安全措施等原则。

个人信息既具有个人财产价值，也具有社会公共价值和商业价

值。推动用户个人信息保护工作，要考虑个人信息的多种属性，实现基于安全可控基础上的合理使用和恰当平衡。这一点已经成为全球各国的普遍共识，并且反映在立法中。《加州消费者隐私保护法》着力突出“所有权赋予、安全保护、个人控制”三点；欧盟《一般数据保护条例》体现了包容性监管思路，推动信息保护和促进数据资源的合理规范使用，为行业自律留下了空间。

二、用户个人信息保护的国际形势

（一）用户个人信息保护面临严峻态势

随着信息通信技术的应用普及，网络数据流转通道逐渐扩大，网络上流通的个人信息愈加广泛，全球个人信息安全问题日益凸显，盗取数据资源谋求商业利益的行为日益增多，形成了明显的黑色或灰色产业链。这类行为与用户权益联系紧密，轻则导致公民财产损失，重则危害行业发展，挑战监管底线。美国电信运营商 Verizon 发布的《2018 年数据泄露调查报告》显示，网络犯罪所窃取的个人信息主要有支付细节、医疗记录、凭证等，这类事件主要集中在健康医疗、住宿和餐饮业、公共服务等领域。

近年来，众多全球知名企业发生个人信息泄露事件。2017 年，亚马逊公司 AWS 云存储库 47G 的医疗数据意外对公众开放，导致 15 万患者的姓名、住址、病例记录、检查结果等重要信息遭到泄露。同一年，征信企业 Equifax 遭遇黑客攻击，导致 1.43 亿用户的个人信息

被泄露，其中包括姓名、社会安全号、住址、驾照号、社保号、信用卡号等重要内容。2018 年 3 月，美国著名运动装备品牌 Under Armour 旗下一款食物和营养主题应用“My Fitness Pal”的 1.5 亿用户数据被泄露，包括用户名、邮箱地址和加密的密码。2018 年初，Facebook 将 5000 多万用户的信息提供给英国剑桥分析公司一事更是引发全球关注，上升到国际政治层面。多种原因导致了该类事件的频繁发生：

一是个人信息外延的扩大。技术发展让个人信息的外延扩大，一切能识别、关联和反映到特定个人的信息都纳入个人信息范畴。海量数据的流转往往裹挟着大量的个人信息，使其边界日益模糊，增加了保护难度。

二是技术发展的负外部性。人工智能、云计算等新技术的发展在更加依赖于数据资源的同时，不可避免的带来了负外部性，加大了个人信息的安全风险、冲击了个人信息保护体系。例如，勒索软件和恶意代码通过电子邮件、入侵服务器、攻击供应链、挂马网页、系统漏洞传播等方式盗取个人信息。

三是监管模式的滞后。产业链的延长、市场主体的增加让个人信息的多向流动成为常态，使得个人信息安全的监管牵扯到多个行业、多个领域，导致监管目标和监管任务难以区分，冲击了传统监管体系，提升了监管难度。

（二）欧盟、美国及日本形成三种典型保护模式

当前，欧盟和美国代表了最具影响力的两种个人信息保护模式，

前者以政府主导下的严格立法和统一监管为主，政府规制起到了核心作用；后者体现为行业驱动与规则塑造下的多方博弈，行业自律与政府有限干预相互结合。在亚太地区，日本的经验同样具有代表性。

1. 欧盟模式：政府主导下的严格立法和统一监管

GDPR（《一般数据保护条例》）是欧盟个人信息保护的核心法律。GDPR 具有强制实施效力，构建了一套完善的个人信息保护体系，能够直接适用于欧盟全境。在保护范围上，个人信息的外延得到延展，医疗健康、生物标识等都成为保护对象。在用户权利上，GDPR 引入被遗忘权、可携带权、删除权等新型权利，与知情权、同意权、访问权、反对权等共同构成用户享有的基本权利类型。在隐私政策制定上，企业必须确保“隐私设计”（Privacy By Design）的原则贯穿到整个数据处理过程中，在产品和服务的全业务周期流程中做到保护个人信息安全。在数据控制者的义务上，GDPR 设计了隐私影响评估、数据泄露预警和业务流程记录等要求，可以理解为数据控制者必须采取“足够的措施”来确保数据安全。总的来看，GDPR 赋予用户充分的个人信息自决权，而企业及其他掌握数据资源的主体必须承担更多的义务。从产业链条的逻辑来看，整个数据链的上下游各利益主体都会被问责，实现全方位的保护。

GDPR 设立“联盟-机构-国家”三级监管体系，通过统一监管、一致协调、各自实施确保各个条款的具体落实，有助于建立“一站式”的争议解决和服务流程，逐步消除各国个人信息水平不一致的碎片化现状。在监管机构设置上，GDPR 设立欧盟数据保护委员会（European

Data Protection Board，简称 EDPB）来确保 GDPR 执法过程的统一性和连续性，该机构处于欧盟数据保护体系的中心位置，协调各国数据保护机构合作；在人员构成上，EDPB 由各国数据保护机构和欧盟数据保护监督员或其代表组成，欧盟委员会有权在不投票的前提下参与其会议，让各国做到充分沟通。具体任务上，EDPB 不仅制定 GDPR 的指南性文件，同时也作为最高裁决者对数据跨境处理等争议发布具有约束力的决定，避免 GDPR 执行过程中因各国司法体系的差异产生混淆。GDPR 还规定，欧盟各实体机构设立数据保护官员（Data Protection Officer，简称 DPO）来监管内部的个人数据处理活动是否合规；从职能来看，数据保护官员相当于机构内部的首席隐私官，其主要作用在于评估潜在的隐私风险并提出针对性建议，目前已经有包括欧洲议会、欧洲中央银行在内的数十个欧盟机构设立了数据保护官员。各成员国的数据保护机构将根据 GDPR 的要求，对境内企业的个人信息处理活动进行监管；各国监管机构必须互通有无，如出现分歧将提交欧盟处理。

2. 美国模式：行业驱动与规则塑造下的多方博弈

美国模式中，政府和企业呈现出充分合作、灵活博弈的关系。政府十分重视市场调节作用，通过对行业组织赋权并支持其开展管理活动，发挥行业自律的作用。美国的个人信息保护主要有以下几点：

一是基于总体原则下的分散立法。美国并没有统一的个人信息保护法，而是通过在联邦层面为个人信息保护工作提供宏观依据，主要体现在《公平信息实践法则》《隐私法》等联邦法律中；同时在重点

领域进行立法，如《电子隐私通信法》《儿童在线隐私保护》等联邦法律，以及《加州消费者隐私保护法》等地方法律。

二是高度重视行业自律。行业自律的典型代表是行业认证，主要由民间组织、技术团体等私营机构主导，通过制定个人信息保护标准并开展认证和授权工作，主要包括法律授权、企业评估、行业认证、事后争议解决等，实现“政府搭台、企业唱戏”，带动用户个人信息保护水平提升。总部位于加州的个人隐私认证机构“TRUSTe”是这方面的代表。

三是两大委员会是监管主角。美国的电信和互联网用户个人信息保护监管主要由联邦通信委员会和联邦贸易委员会负责，前者主要针对电信用户，后者则聚焦于互联网用户。二者在监管触发机制和监管手段上较为相似，主要针对企业隐私政策、用户举报、数据泄露等，监管手段包括约谈、发函、调查、庭外和解、罚款等。

3. 日本模式：政府主导+行业自律混合模式

日本的个人信息保护有其独特经验，其个人信息保护立法主要参考欧盟，行业规范主要依据美国，通过“政府主导+行业自律”混合模式充分发挥地方公共组织和行业协会的作用。该国《个人信息保护法》也体现了充分的行业自律空间，兼具欧美所长。

一是立法的全面性。《个人信息保护法》等“关联五法案”构成了个人信息保护的核心制度；多数地方政府和大量公共团体制定了个人信息保护条例。

二是监管的独立性。根据《个人信息保护法》成立的个人信息保

护委员会具有高度的独立性，拥有监督、处理申诉、保护评估、向国会报告等独立权力。

三是行业的自律性。根据“一般财团法人日本情报经济社会推进协会”（Japan Institute for Promotion of Digital Economy and Community，简称 JIPDEC）出台的《个人信息保护管理体系要求事项》构建了行业个人信息保护管理体系的和认证工作（P-MARK 认证），通过认证的企业将获得相关标识。

四是体系的完备性。《个人信息保护法》给企业留下充分的行业自律空间，政府指导开展行业认证工作，体现了“政府主导+行业自律”的灵活性。

对比三种典型模式，欧盟模式基于统一的立法和监管对个人信息进行严格规范，强调政府力量的作用，具有强制的约束力和价值观输出，但会造成企业合规成本过高，一定程度抑制了产业发展；美国模式依托于其强大的信息通信业实力与全球布局，强调产业力量的作用，凸显政府、企业、用户等不同主体间的利益均衡，但对市场成熟度有很多要求，并且不同地区保护水平存在不一致；日本模式从表明看相对更加合理，但对相应的政策和市场制度设计、实施、保障等提出了更高要求。总的来说，一个国家的个人信息保护模式与其经济社会发展、产业发展路径、数据安全需求“一脉相承”，需要遵循立法公正、经济合理、司法可行的原则，选择适合实际国情的。

（三）用户个人信息保护的国际间规则积极推进

从 1980 年至今，个人信息保护的国际间规则主要经历了三个阶段，内容也从早期的原则性沟通逐渐集中到数据跨境传输领域。其内容演变，既是行业发展的客观要求，也是政治博弈的必然结果。

第一个阶段的代表是 OECD《保护隐私和个人数据跨境流动指导原则》（简称 OECD 指南）和欧洲委员会《个人数据自动化处理的个人信息保护公约》（简称 108 号公约）。这两份文件规定了个人信息处理的基本原则，包括有限信息收集、数据质量、特定目的、安全措施、公开问责等，成为个人信息保护立法的重要依据。2013 年，OECD 对指南进行了微调，增加泄露通知、集体诉讼等内容。

第二个阶段的代表是 APEC 跨境隐私规则体系（Cross-Border Privacy Rules，简称 CBPRs），也是亚太地区唯一的数据跨境传输规则。目前已经加入 CBPRs 的有美国、加拿大、日本、韩国、墨西哥和新加坡，取得认证资质的机构有美国的 TRUSTe 和日本的 JIPDEC，截至 2018 年有 20 多家企业通过认证。为确保该体系顺利实施，APEC 设立了跨境隐私执法安排机制（Cross-border Privacy Enforcement Arrangement，简称 CPEA）作为执法机构跨境执法、信息共享的平台，由美国联邦贸易委员会和日本个人信息保护委员会主导，目前共有 27 个机构参与，包括我国香港的隐私专员公署和台湾地区的数个部门。从主导力量和参与数量来看，该机制处于“半搁浅”状态，这是因为该机制由美国主推，参与方多为美国盟友，参与方必须修改本国法律以达到 CBPRs 的要求，这一做法既不符合亚太地区经济体的利

益诉求，又带有一定的政治捆绑成分，因而推进缓慢。

第三个阶段的代表是欧盟与美国的隐私盾（Privacy Shield）协议和欧盟GDPR的约束性公司章程（Binding Corporation Rule，简称BCR）。“隐私盾”是欧盟与美国数据传输的双边规则，为平衡欧盟与美国在数据资源获取能力上的差异。该协议赋予欧盟委员会针对美国政府的审查权，同时给予欧盟公民一定的救济权利，以制约美国政府监控和获取欧盟公民信息。BCR是为企业设立的内部数据自由流动规则，允许跨国公司内部实现数据自由传输。该机制的设计避免了传统监管模式为数据跨境传输设立前提条件，调动了市场主体参与监管工作的积极性，是合作性治理模式的典范。截至2018年8月底，已经有超过百家企业获准通过BCR，其中包括斯伦贝谢、壳牌、道达尔、空中客车、英国电信等知名跨国公司。

此外，一些国家的立法也不可避免的涉及个人信息跨境处理。2018年初，美国通过的《澄清境外数据的合法使用法案》（Clarify Lawful Overseas Use of Data，简称Cloud法案）对执法机构调取别国个人信息进行了规定，同时允许“适格”外国机构调取美国公民信息，判断基准是“外国政府的立法和国内法执行是否给予隐私和公民权利提供了稳健的保护”。从条件看，满足“适格”标准的多数是美国盟友。欧盟GDPR将“充分性标准”作为与域外国家实现数据自由流动的前提，推动数据跨境流动规则“向欧盟看齐”，这一举动旨在推广欧盟的个人信息和数据治理规则，将更多经济体拉入到欧盟的数字市场中。

三、用户个人信息保护的国内现状

（一）我国已初步建立个人信息保护体系

总体来看，我国已经初步建立了与国内环境相符、与全球态势相适的个人信息保护体系。法律法规方面，《民法总则》《刑法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》《网络安全法》《电信和互联网用户个人信息保护规定》等逐步形成个人信息保护法律框架；标准方面，《个人信息安全规范》等国家标准及系列行业标准推动标准体系日臻完善；监管方面，以“查证、管理、处罚”为主要手段，管理部门依法履职持续加大监督力度；行业方面，企业积极探索和提升保护能力，行业组织加快推进行业自律工作；用户方面，自我保护意识不断提高，对保护工作提出更高需求。

与此同时，我国的个人信息保护依然存在诸多问题。在大数据时代，个人信息收集、使用和流转涉及多个流程、多个主体，容易被不法分子窃取、传播、交易，严重危害用户的人身安全、财产安全以及社会安全。2017 年下半年，辽宁省破获的特大侵犯公民个人信息案，涉及逾百亿条个人信息；2018 年 8 月，华住集团旗下的连锁酒店约有 1.3 亿住客的信息被泄露，共计 5 亿条，包括姓名、手机号、身份证号、家庭住址等。根据最高人民检察院发布的《侵犯公民个人信息犯罪典型案例》，侵犯公民个人信息犯罪正在与电信网络诈骗、敲诈勒索、绑架等犯罪呈合流态势，社会危害更加严重。上述事件表明，提升用户个人信息安全水平任重而道远。

（二）立法及标准相继出台

1. 用户个人信息保护法律制度框架逐步形成

我国的个人信息保护立法属于分散模式，专门性的个人信息保护法尚未出台。《宪法》作为国家根本大法规定了“中华人民共和国公民的人格尊严不受侵犯”。这里的“人格尊严”即公民的人格权，指的是与人格价值有关的基本权利，例如隐私权。早期立法主要通过保障“个人隐私”或“个人秘密”来实现对个人信息的间接保护，如《侵权责任法》《民事诉讼法》《计算机信息系统安全保护条例》等法律、行政法规中的相关内容。

在民事上，2017 年生效的《民法总则》明确提出保护公民的“个人信息”和“隐私权”；2014 年实施的《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》确定了个人信息的法律内涵及侵权责任承担方式。

在刑事上，《刑法修正案（九）》将《刑法修正案（七）》的“出售、非法提供公民个人信息罪”和“非法获取公民个人信息罪”整合为“侵犯公民个人信息罪”，放宽了该项罪名的成立条件；2017 年生效的《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》将反映特定自然人活动情况的各种信息，例如行踪轨迹信息等纳入个人信息保护范围，明确了量刑标准。

2012 年生效的《全国人民代表大会常务委员会关于加强网络信

息保护的决定》、2013 年生效的《电信和互联网用户个人信息保护规定》、2017 年生效的《网络安全法》等法律法规界定了电信和互联网行业用户个人信息保护的概念，提出了具体的保护措施和罚则。

2. 用户个人信息标准日臻完善

我国的用户个人信息保护国家标准主要是推荐性标准，以 2018 年正式实施的《信息安全技术 个人信息安全规范》（简称《个人信息安全规范》）为代表。在《网络安全法》的框架下，《个人信息安全规范》界定了个人信息的内涵和外延、规范了个人信息处理原则，就个人信息控制者在个人信息的收集、保存、使用、委托处理等过程中的操作规范和应守准则提出了具体要求。在现有法律法规过于原则性的前提下，该规范弥补了许多操作性空白，为优化政府监管、推动企业合规提供了符合行业发展需求的规范性指引，同时为后续标准制定及立法提供了重要参照。

在行业标准方面，全国通信标准化服务委员会下属的用户个人信息保护标准工作组正在推动“电信和互联网服务个人信息保护标准体系”的构建，目前已完成《电信和互联网服务 用户个人信息保护 定义及分类》《电信和互联网服务 用户个人信息保护 分级指南》《电信和互联网服务 用户个人信息保护技术要求 移动应用商店》《电信和互联网服务 用户个人信息保护技术要求 即时通信服务》《电信和互联网服务 用户个人信息保护技术要求 电子商务服务》五项行业标准的制定。该体系首次从电信和互联网服务质量角度出发，对用户个人信息保护提出定义、分类、分级和管理技术要求，对移动应用等重

点服务提出了个人信息保护规范指引，对促进行业自律起到了积极推动作用。

（三）监管机构依法履职开展各类监管行动

履行个人信息保护监管的机构主要有全国人大常委会、中央网信办、工信部等。全国人大常委会根据自身职能履职，对法律实施情况进行监督检查；中央网信办根据《网络安全法》统筹协调网络安全工作和相关监督管理工作；工信部和省级电信管理机构根据《电信和互联网用户个人信息保护管理规定》等开展行业内的用户个人信息保护工作。

全国人大常委会依法履职开展“一法一决定”执法检查。2017 年下半年，全国人大常委会执法检查组开展了针对《网络安全法》《全国人大常委会关于加强网络信息保护的决定》实施情况的专门性检查，包括公民个人信息保护制度落实情况、查处侵犯公民个人信息相关违法犯罪情况等。从检查结果看，我国近年来出台了一批涉及个人信息保护的法律法规，针对侵犯个人信息犯罪高发态势采取的专项行动，打击利用公民个人信息实施的电信网络诈骗犯罪，侦破了大量该类案件，取得了良好的法律和社会效果。与此同时该项工作依然面临诸多问题，例如手机免费程序普遍存在过度收集用户信息和侵犯个人隐私的现象；一些互联网公司和公共服务部门存储的大量公民个人信息由于安防技术落后容易被盗取；一些地方形成了非法收集、窃取、贩卖和利用公民个人信息的黑色产业链。这些都是下一步工作亟待解

决的顽疾。

中央网信办牵头隐私条款联合检查。2017 年，中央网信办与工信部等三部委联合开展了“隐私条款专项行动”，对微信、微博、淘宝、京东商城、支付宝、高德地图等十余款网络产品的隐私条款进行评审。本次行动希望对代表性网络产品的隐私条款进行专门性梳理和分析，督促网络运营者提升个人信息安全保护水平，做到树立标杆、提升影响，带动个人信息保护水平提升。从评审结果来看，十款产品在隐私政策方面均有不同程度提升，做到了明示收集、使用个人信息的规则，并征求用户明确授权，其中个别产品还做到了向用户主动明示并提供更多选择权。

工信部以正面引导和问题查处为抓手开展行业用户个人信息保护监管。前者可以概括为“引导、推进、提升”，主要目的是形成示范效应，通过专项行动、政策讨论、舆论宣传等方式凝聚共识，引导行业自律、提升用户意识。例如，工信部在“5•17”世界电信日、全国网络安全周等加强宣传教育，希望引起各界关注。后者可以概括为“查、管、罚”机制，通过日常监管、行风检查、季度拨测、感知调查等方式，包括制度查阅、技术检测、现场检查、用户调研等手段，对发现的问题做到及时约谈、责令整改、后续监督。2018 年初，工信部约谈了百度、今日头条、蚂蚁金服等互联网企业，就用户协议默认勾选、使用目的告知不明确等问题进行了通报并要求整改，维护用户合法权益。

（四）企业从理念到操作提升个人信息保护能力

部分企业积极探索多种方式，从理念到操作上提升个人信息保护能力。从商业利益来看，用户个人身份和行为信息涉及商业利益，是重要的数据资产，保护个人信息安全就是保护企业数据资产完整。从社会责任来看，保护用户个人信息安全能够有效降低泄露、非法倒卖个人信息等行为的发生，净化市场秩序、提升企业信誉。

基于“隐私设计”的个人信息保护体系。“隐私设计”是在全生命周期流程贯彻积极的隐私保护理念，强调企业的主动参与和用户可控，使得个人信息既不受非法侵犯又能得到合理使用。这一理念要求企业在新技术、新产品的最初阶段就要考虑隐私和安全，通过主动推进、而非被动补救的方式来确保个人信息安全与合理使用。在国内实践上，部分企业将其称为“默认隐私”，认为个人信息保护不仅存在于技术层面，也涉及到法律、流程、管理、产品涉及等层面。目前，部分领先企业已经在系统架构改造等环节实施这一理念，技术上实现了数据全链路加密，并且通过建立隐私保护小组对产品实行“安全+隐私”的双评估。可以看出，“隐私设计”是一个动态的概念，需要根据技术水平和商业模式来灵活调整。

根据政策和市场及时更新隐私政策。企业的隐私政策能够体现个人信息保护理念，主要说明信息收集的内容、用途、用户享有的权利、适用范围等，通常与公司的用户服务协议紧密相连。可以说，用户可以通过隐私政策了解企业如何收集、使用、分享、删除个人信息，进而做到对个人信息进行有效管理。企业通常会根据政策导向、监管

变化、行业发展等更新隐私政策。2017 年“隐私条款专项行动”后不久，多数企业陆续更新了隐私政策，做到了提示更明显、描述上更加通俗、操作性更强。在用户提示上，有的企业通过弹窗提示的方式告知用户已更新隐私政策；在用户信息管理上，有的企业新条款详细写出了操作路径来指引用户；在用户信息使用上，有的企业罗列了第三方合作伙伴类型及共享的用户信息内容。

技术手段与用户赋权并行。提升个人信息保护能力，既要采用最新技术手段，也要通过用户赋权来实现个人信息的优化使用。腾讯已经使用了匿名化处理、差分隐私技术来弱化或切断个人信息的可识别性，同时在用户协议中设置选择性加入(opt-in)、选择性退出(opt-out)等选项，做到了商业便利和用户权益的平衡。华为在产品中采用了 virSign（全球最大信息安全数字证书认证）数字证书来验证，同时搭配双层密钥管理方案进行数据加密，保护用户信息从收集、传输到使用各个环节的安全性和完整性。

（五）行业组织多管齐下开展工作

行业机构持续开展个人信息保护技术监测。在工信部指导下，中国信息通信研究院连续多年针对互联网信息服务、手机应用软件等用户个人信息保护情况进行业务拨测、真实数据测试、技术检测和行为取证，发现的违规应用软件通过工信部电信服务质量通告向全社会公开，并逐步建立部、省联动机制，加强政府监管。国家互联网应急中心（CNCERT）持续监测互联网恶意应用软件，对监测发现的恶意

样本定期对外公布。

全国信息安全技术标准化委员会（TC260），中国通信标准化协会（CCSA）等标准组织积极开展个人信息保护标准制定。TC260 组织制定了《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》《信息安全技术个人信息安全规范》等多项国家推荐标准。中国通信标准化协会（CCSA）为保证电信和互联网用户个人信息保护工作有效开展，依托 TC543 和 TC485 开展了电信和互联网服务用户个人信息保护、智能终端个人信息保护、大数据信息安全等国家和行业标准的制定工作。

众多企业、研究机构聚焦个人信息保护主题成立联盟、工作组等行业组织，期望通过行业自律共同推动个人信息保护水平提升。中国互联网协会成立个人信息保护工作委员会，提出了组织制定行业规范和标准，促进行业协作和预警机制建设，实施社会和公众监督等多项工作任务，电信运营商、移动社交、电商、搜索引擎、终端制造等领域的近百家企业加入工作委员会。数据中心联盟成立用户数据和权益工作组，旨在搭建个人信息和权益保护行业交流研讨平台，推进个人信息保护标准研究制定，识别和解决行业个人信息保护问题，开展用户数据和权益保护可信评估，推动电信和互联网服务用户个人信息和权益保护行业自律，目前已有 30 余家电信和互联网企业深度参与工作组工作。此外，移动安全联盟（MSA）、电信终端产业协会（TAF）等行业组织均已启动个人信息保护相关的技术研究、标准制定、评估评测、社会监督、自律公约等工作。相关联盟协会的工作有效补充了政府监管工作，行业自律的方式将有效激发企业个人信息保护积极

性，迅捷的行业信息共享有助于快速应对新型技术带来的潜在安全隐患，由点及面的牵引作用将拉动行业个人信息保护水平的整体提升。

（六）用户对个人信息保护需求强烈

中国信息通信研究院调查发现，广大用户的个人信息安全感知评分不高，重点问题突出。2018 年上半年的用户个人信息安全感知评分仅为 6.3 分（调查采用 10 分制评分，分值越高，说明安全性越高），较 2017 年同期（6.5 分）下降了 0.2 分，较 2013 年同期（6.4 分）下降了 0.1 分，总体现状不容乐观，长时间以来用户对个人信息保护的获得感停留在较低水平，有强烈的安全需求和保护诉求。

从反映的重点问题来看，有 39.9%的用户认为企业存在“未经用户同意擅自向他人提供个人信息”，有 28.1%的用户认为企业“收集过多不相关的个人信息”，有 25.3%的用户认为企业非法出售个人信息；其他反映突出的问题包括未经用户同意自行使用个人信息、超出授权扩大个人信息使用范围、缺乏有效的投诉渠道等。

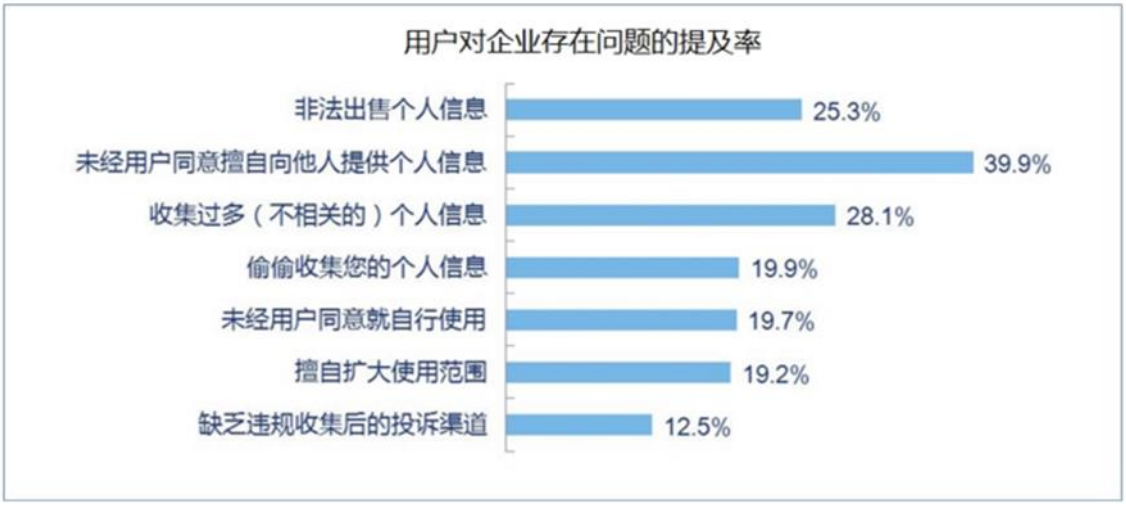

图 1　用户认为企业在个人信息保护方面存在的主要问题

与此同时，用户自身也存在个人信息保护意识和能力不足。有些用户个人信息安全意识淡薄，如在银行卡、社交网络等应用的密码设置过于简单，容易被破解；或者随意扫描二维码、浏览安全性不确定的网页，为个人信息泄露埋下隐患；一些用户不熟悉用户服务协议中涉及个人信息的内容，也不清楚如何向监管机构、消费者组织、企业客服等渠道反映问题，维护自身合法权益。

用户作为个人信息保护的关键环节，在多方协同保护框架下，一方面相关部门及企业需要着力加强对用户的网络信息安全教育，如制作用户安全手册、推动安全知识普及，提高用户自身安全防护意识与能力；另一方面需要构建完善用户参与机制，让用户不仅是受保护的对象，还要发挥用户在个人信息保护中的积极作用。

四、国内个人信息保护典型案例与特征

用户个人信息关系个人和社会的核心权益及安全，也是数字经济时代重要数据资产和关键生产要素，具有强烈的保护要求和利用诉求。现实中，个人信息在收集、传输、存储、使用、流通等各环节，由于保护与发展的不均衡，导致诸多保护问题频发。通过典型案例及应用行为分析，洞察其中的问题特征及原因，为更好地开展保护工作、促进保障安全的同时科学合理利用，提供方向和参考。

（一）典型案例分析

用户个人信息泄露或违规提供，Facebook（脸书）事件影响未

来数据保护形势。2018 年 3 月，媒体曝光了 Facebook 超过 5000 万用户的个人信息被英国剑桥分析公司用于定向投放政治广告，影响 2016 年美国总统选举。事件发生后，美国国会和欧洲议会先后举行听证会，就 Facebook 如何处理用户数据和隐私问题展开参议员质询；美英等国监管机构就此事件开展了调查，其中，英国信息专员办公室以违反《数据保护法》为由对 Facebook 处以了 50 万英镑的罚款。Facebook 推出了补救措施，包括推出数据滥用悬赏计划提升用户对个人信息的控制力、设置隐私菜单快捷方式来优化隐私条款的告知效果、收紧和规范对第三方合作伙伴管理等。

这一事件将导致全球个人信息保护监管形势趋于严格。从发生时间来看，此事件正值 GDPR 生效前夕，给予了欧盟利好信号，有利于其在全球输出推广个人信息保护标准和价值观，让部分国家的个人信息保护监管向欧盟看齐；美国联邦贸易委员会已经启动调查，不排除出台更加严格的数据监管政策。面对监管收紧，Facebook 已经禁止第三方收集用户敏感信息并且缩小第三方应用可以访问的用户信息范围，保障对数据的控制力、试图将数据流通在平台范围内。其他互联网巨头如果采取类似举措，将影响数据流动、可能形成数据资源垄断，形成欧美国家聚集数据资源的“凹地效应”。我国的互联网企业走出去势必面临获取数据资源的困境，增加开拓海外市场的成本，同时面临数据资源无法向境内回流的困境。

漠视用户知情权和选择权，监管机构加大对侵犯用户隐私的问责力度。2018 年初迄今，一批典型的 APP 应用被曝侵犯用户隐私。支付宝用户查阅年度账单，发现被默认勾选《芝麻服务协议》；手机

QQ 浏览器、手机百度等应用涉嫌偷拍或监听用户；滴滴顺风车业务的乘客司机互评功能，让乘客的隐私全面暴露，增加了安全风险。事件发生后，监管机构启动了问责机制。工信部就个人信息保护问题约谈了支付宝等公司，就存在的个人信息收集和使用规则告知不充分等典型问题进行约谈和通报，要求企业立即整改，充分保护用户的知情权和选择权；交通部、公安部以及多地的交通和公安部门先后约谈滴滴，要求整改顺风车业务，保障乘客出行安全。作为回应，支付宝取消了年度账单的默认同意选项；滴滴公司取消了个性化标签等社交功能，增加了乘客一键报警等安全功能，并且在 8 月份下架了顺风车业务。

在互联网服务中，服务提供商利用相对强势地位，在服务协议中预设用户“默认同意”，侵害了用户的知情权和自主选择权；超授权范围获取不必要的个人信息，不仅超出了商业经营目的，更是给用户的人身安全带来威胁，不利于行业信任机制的建立。《网络安全法》生效以来，国家加大保护个人信息的力度，类似事件更是让监管部门推出严厉的措施，旨在全面落实相关法律法规，通过外部约束让行业形成保护用户个人信息的意识。

个人信息违规收集与使用，“大数据杀熟”拷问个人信息使用的商业伦理。很多机票、酒店、电影、电商平台针对不同用户、不同时间段标注的价格存在差异，并且被默认勾选附加服务，这一现象在业内被称为“大数据杀熟”。例如，老用户看到的价格比新用户要贵，同一用户在预订前比预订后看到的价格要贵。其基本逻辑是，网站会根据用户的个人身份、订单历史、出行轨迹、会员等级等进行精准画

像，通过大数据技术来推算出用户的价格接受程度和出行刚性需求，进而显示相应价格。近期，国务院督察组对电信行业的督查中也指出，电信运营企业存在只对新用户提供优惠、对老用户杀熟的情况。

大数据杀熟的实现，依赖海量数据资源。一些企业往往会超出承诺的服务范围过度收集用户个人信息，并且用算法对这些信息进行深度挖掘后，将结果用于精准营销。监管的滞后和行业自律的缺位，使得大数据杀熟几乎成为了行业“潜规则”。这种行为既涉嫌滥用个人信息，也存在价格歧视的嫌疑，违背了公平自愿、诚实守信的商业原则，违反《消费者权益保护法》《价格法》《电信和互联网用户个人信息保护管理规定》等法律法规。完善用户个人信息收集、挖掘利用方式及算法模型使用规范，并强化打击利用新技术窃取个人信息的行为，加强数据防护水平，探索提升企业违规使用个人信息取证技术能力，是治理“大数据杀熟”的重要基础。

（二）典型应用分析

移动智能终端产业飞速发展，移动互联网正逐渐改变人们的生活习惯和行为模式，各类应用软件对用户个人信息的收集和使用已经成为常态。用户个人信息作为信息服务与用户连接的载体，为信息领域新产品、新服务发展提供了重要支撑。正因为用户个人信息的高价值属性，用户个人信息未经授权即过度采集和滥用的问题愈发严重，智能终端应用软件泄露用户个人信息事件频繁发生，用户个人信息安全处于风险中。

自 2013 年下半年起，中国信息通信研究院对 Android 系统应用软件用户个人信息保护情况进行定期跟踪监测，截至目前已累积监测 170 余家应用商店的 100 万余款应用软件，监测统计结果显示，目前 Android 系统应用软件用户个人信息保护情况不容乐观。

各类型手机应用软件读取用户设备信息行为占比约 80%左右。设备信息包括手机 IMEI、IMSI、手机号码及位置信息等。

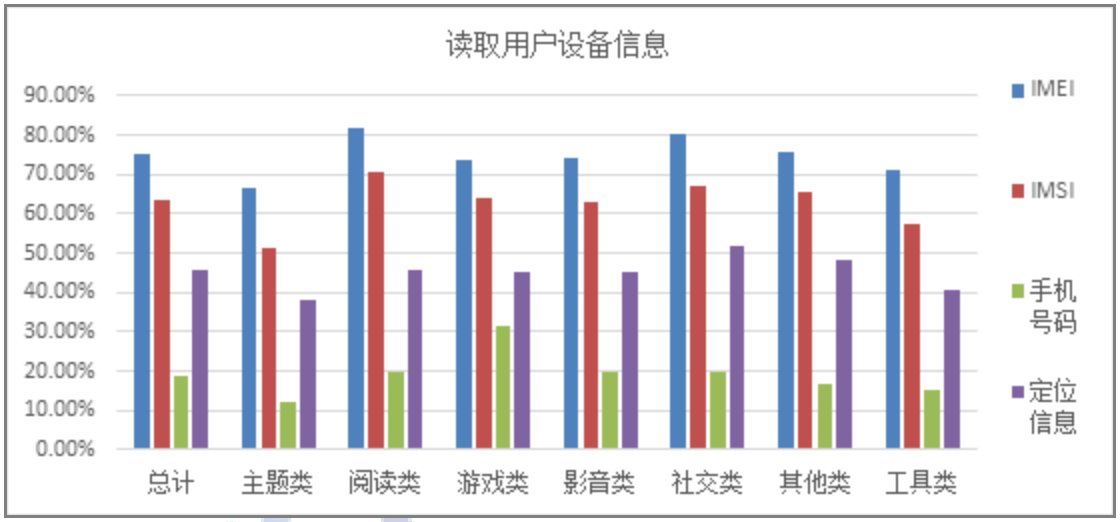

图 2 各类型手机应用软件读取用户设备信息情况

各类型手机应用软件读取用户联系人和通信信息行为占比约 5%[1]。用户联系人和通信信息包括用户通讯录、通话记录、短信记录等信息。

[1] 此处指实际真正读取了用户终端通讯录或者短信记录的行为，而不是指获取用户终端通讯录权限，很多应用获取了通讯录权限，但是并没有实际读通讯录的行为。

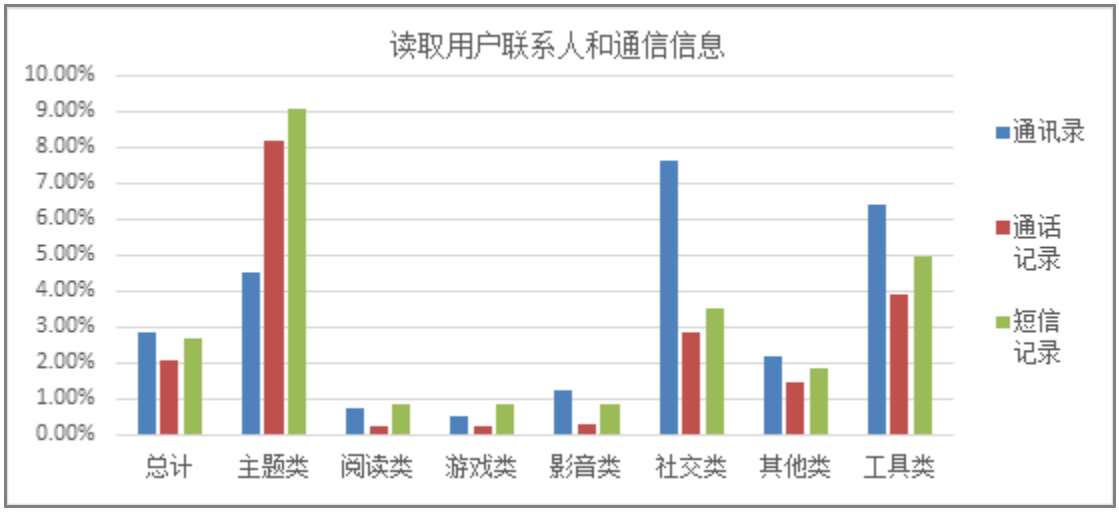

图 3 各类型手机应用软件读取用户联系人和通信信息情况

各类型手机应用软件读取用户系统信息行为占比约 50%左右。用户系统信息包括用户手机应用安装列表、音视频列表、手机系统日志等信息。

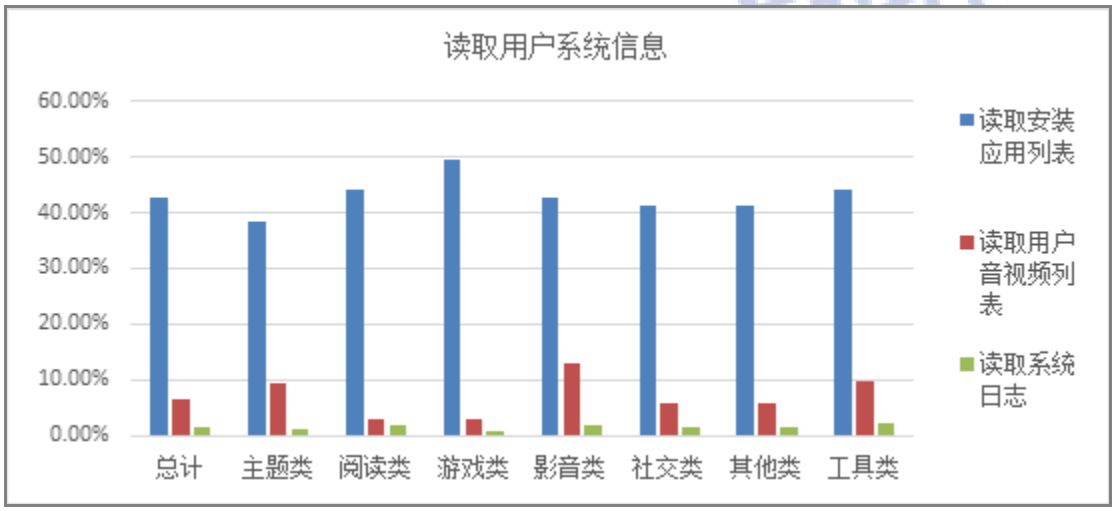

图 4 各类型手机应用软件读取用户系统信息情况

各类型手机应用软件植入广告或权限存疑（申请权限与实际使用不符）行为占比约 95%左右。

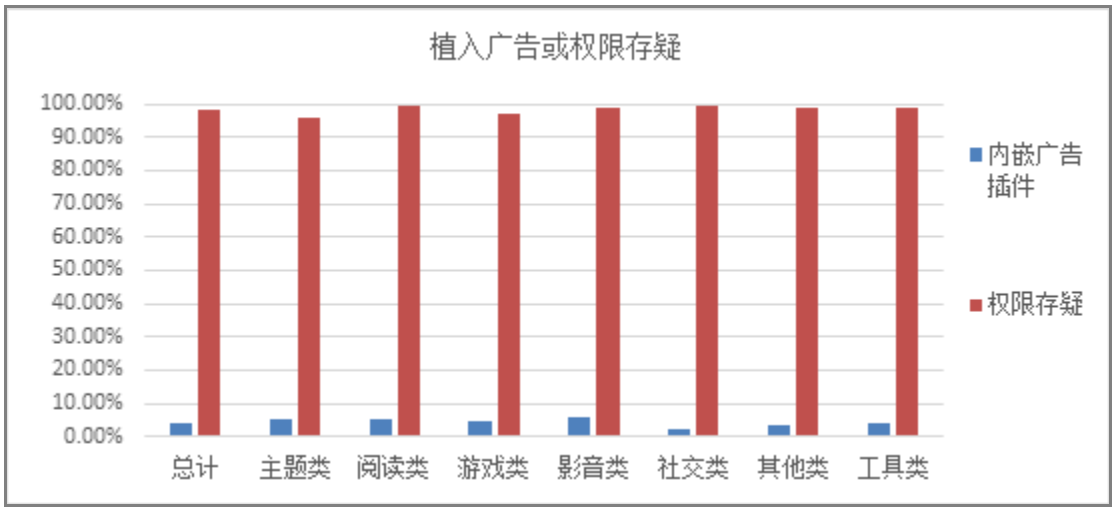

图 5 各类型手机应用软件存在植入广告或权限存疑行为情况

结合监测统计结果以及对部分应用软件的针对性检测分析发现，手机应用软件在用户个人信息保护方面的重点问题包括以下几方面：

一是权限调用不全为服务所必需。工具类、社交类应用软件可以因为服务必要获取用户位置信息，然而监测发现大量阅读类、主题类、影音类应用软件在没有提供位置服务的情况下获取用户位置信息，部分应用软件存在调用提供服务不需要的相关权限行为。

二是部分应用软件调取手机权限未经用户允许。监测发现部分应用软件在调用手机通讯录、位置信息等权限时未明确提示用户，部分应用软件存在用户不知情情况下获取用户个人信息现象。

三是部分应用软件私自将用户通讯录及位置信息发送到远端服务器。监测发现部分应用软件获取用户通讯录及位置信息后，未经用户允许即将用户个人信息传送至远端服务器。

工业和信息化部将手机应用软件用户个人信息保护问题作为《工业和信息化部关于电信服务质量的通告》的重要组成内容对外通告，从 2014-2018 年上半年，问题应用软件总体处于下降趋势，体现了行

业环境的改善和政府监管工作取得积极成效，但“未经用户同意，收集、使用用户个人信息”“恶意吸费”“强行捆绑推广其他应用软件”等行为仍频繁发生，亟需进一步强化行业监管和自律。

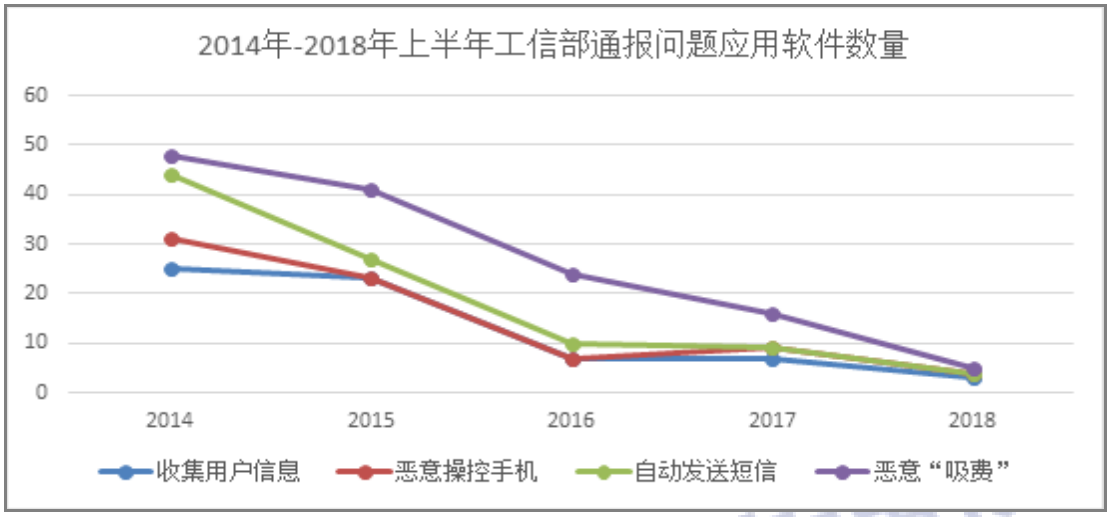

图 6 2014-2018 年上半年工信部通报问题应用软件情况

其中，“强行捆绑推广其他应用软件”占比最大，达到 84%。“未经用户同意，收集、使用用户个人信息”“恶意吸费”等违规应用软件占比相对平均，间接体现出恶意应用软件市场“打擦边球”生态，恶意软件仍然较为泛滥，严重侵犯用户个人信息或财产安全的应用软件在监管打击和市场自律的作用下逐渐减少。

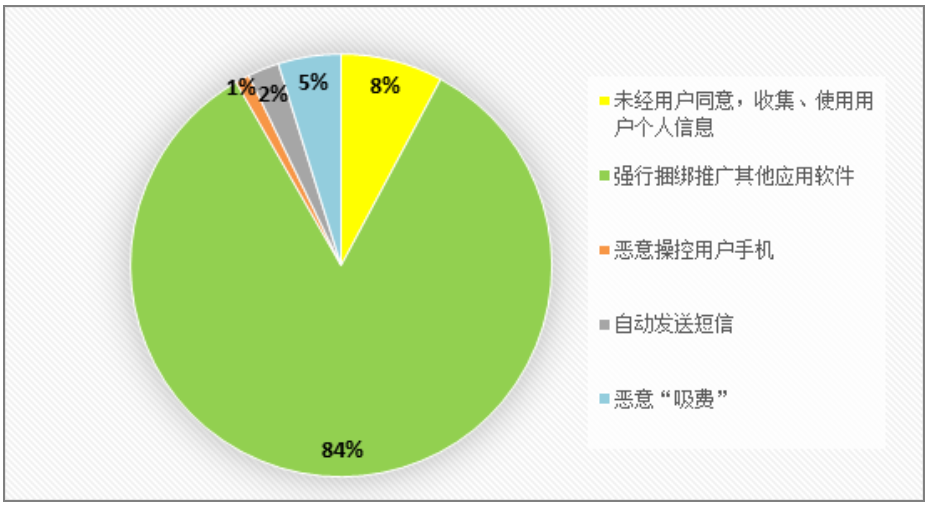

图 7 2014-2018 年上半年工信部通报各类问题应用软件占比

（三）问题特征研究

一是感知层面智能设备的普及和多样化放大了个人信息收集的安全风险。智能手机、可穿戴设备、机器人、物联网传感器等智能设备日益普及，个人信息收集方式更加多样，安全风险进一步放大。因智能终端种类众多且尚未形成统一安全标准，过度收集个人信息成为常态；海量智能设备接入网络，黑客通过漏洞攻击可以盗取更广泛的个人信息；大量应用软件未经安全审查便上线分发，软件漏洞将可能直接造成用户个人信息违规滥用。新一代信息技术在为消费者带来更加智能和便捷服务的同时，必然收集了更大范围的个人信息、开展了更深层次的关联分析、进行了面向更多主体的数据流通，个人信息保护难题凸显。

二是网络层面数据传输量巨大，传输安全存在隐患。大量数据在网络节点的传输加大了引起网络拥塞的可能性，不仅会影响数据的传输效率，同时还会引起网络攻击。存储在关键基础设施的个人信息一旦遭遇网络攻击，将严重影响国家安全、公共利益和个人权益。通过近些年的趋势来看，能源、交通、金融、旅游等重要行业的数据传输量正逐年增加，而大数据传输并未形成统一标准，加大了数据安全传输隐患。

三是应用层面新技术的涌现挑战个人信息流通安全。以自动驾驶、人工智能等为代表的新技术改变了信息的收集、存储和传播方式，给个人信息流通的安全管控带来了新的风险。高精度算法让大量已经去除身份特征的匿名数据重新恢复了身份属性，进而关联到特定个

人，弱化了匿名化技术的效果。伴随新型信息技术的规模化应用，海量的数据源将被深度挖掘利用，个人信息边界的模糊将对各方加强个人信息保护带来难题，个人信息流通环节的安全性和完整性亟需通过新型技术手段加以保障。

四是商业层面企业收集使用个人信息存在泄露隐患。众多个人信息泄露、违规使用等事件表明，一些企业在用户个人信息收集阶段尽量收集更全面的个人信息，甚至通过隐瞒用户的手段窃取用户个人信息，进而通过数据挖掘等技术进行更准确的用户行为画像，催生“精准广告推送”“精准信息流分发”“个性智能化服务”等业务形态。部分企业对个人信息的保护未引起足够重视，长期游走在政策边缘、甚至无视法律法规监督，使收集使用的个人信息面临极大的泄露风险。同时，法律法规不健全、技术标准指引不完善等也是企业个人信息保护难以达到安全要求的客观因素。

五、发展建议

个人信息保护，是构建数字生态系统的前提。个人信息保护水平的提升，体现在立法完善、监管创新、技术突破、企业实践、用户感知等方面。要充分认识到我国个人信息保护工作与全球总体趋势的一致性和自身的独特性，既要实现与国际规则衔接、又要符合国内发展特点。个人信息保护具有多主体、跨行业的特点，要提高思想认识、把握关键原则、多种路径完善治理、探索新型技术应用，调动各方积极性，建立健全开放、协作、高效的多方参与的综合保护体系。

（一）提高个人信息保护的思想认识

个人信息保护是建设数字中国的重要基础。数字中国已经上升为国家战略。这一战略的布局需要整体性的数据资源建设和安全可信的数字环境。完善的个人信息保护体系，是推动数据资源互联互通、构建安全可信数字环境的前提。从这个角度讲，个人信息保护为数据资源合理流动保驾护航，推动数据资源开放共享，释放数据资源价值。

个人信息保护是确保数据资源完整可用的重要保障。个人信息的外延愈加多元，广泛存在于关键信息基础设施和信息化系统之中，是海量数据资源的重要组成部分。保护个人信息的完整可用，就是保护数据资源完整可用，为各行各业的数字化发展提供充裕的生产资料，让个人信息的社会公共价值和商业价值得到充分发挥。

个人信息保护是企业可持续发展的必由之路。中国互联网的发展已经告别草莽时代的野蛮生长，企业做大做强要通过可持续增长路径。企业商业模式的转型，既来源于技术驱动，更是基于用户需求。保护个人信息安全，能够赋予用户充分的安全感，让数据资源创造更多价值，塑造安全可信的商业品牌。

（二）把握个人信息保护的关键原则

既要积极保护也要合理使用。保护个人信息不代表拒绝使用，更不意味着隔离限制。拒绝个人信息使用固然可以杜绝安全风险，但因噎废食意味着数据产业无法发展，与服务用户的目的背道而驰。数据的依法有序流动将提升算法分析能力，能够更好的捕捉风险点、提升

安全保护能力。推动个人信息保护，既要回应大众对隐私权的关切，也要满足企业对数据资源的合理需求，在立法出台和政策落实上做到充分弹性。

要完善保护制度的基本准则。用户个人信息保护制度是保护工作的依据和基础，要完善保护制度的基本准则，为参与各方设立底线。**一是知情同意规则**，切实保障用户作为个人信息主体的知情权和选择权，同时通过创设新型权利、细化行为规范、增加替代方案等增强该规则的灵活性和张力；**二是免除适用规则**，数字经济时代，强调个人信息主体的个人利益和私权保护的同时，需兼顾国家和社会公共利益，设定特殊情况免除个人信息控制者或处理者某些限制和义务；**三是风险管控规则**，引入基于风险管控的保护制度设计，从收集使用个人信息的性质、范围、环境、目的以及对个人的权利带来风险与损害的可能性和严重性出发，根据个人信息保护的情景与可能风险，强化个人敏感信息的保护，重视个人一般信息的利用；**四是侵权救济规则**，针对频繁的个人信息权利被侵犯问题，必须完善民事、刑事、行政等救济制度及措施，加大对侵权行为的打击和惩处力度，保护用户的合法权益。

要防止实操过程中过于形式化。当前的个人信息保护规则很大程度上参照欧美，带有明显的“非工具化”特点，重视价值导向、缺乏统一的操作标准。《网络安全法》等法律法规，规定了知情同意、最少够用等基本原则，要结合具体场景并通过调整才可以落地。要鼓励企业优化数据治理机制、探索技术与管理措施，采取与风险程度相适、与应用场景相符的个人信息保护方式。

（三）多种路径完善个人信息保护体系

完善落实法律保护制度。现有用户个人信息保护法律法规原则性较强、可落地性偏弱，须针对性的制定相应的实施细则，从技术标准和管理要求两方面加强。积极推动出台个人信息保护法，进一步规范个人信息收集、使用行为以及安全防护，明确用户享有的基础性和派生性权利、企业应当履行的义务、各监管机构应当承担的职责等，为政府监管提供详实可靠的依据。企业在实施过程中，应基于自身技术能力和商业模式，做到对法律法规和行业标准的灵活应用，形成符合自身特点的个人信息保护模式。

树立包容审慎的监管理念。要将个人信息保护作为创新行业监管方式的重要领域，要着力营造规范有序、包容审慎、鼓励创新的发展环境，统筹好发展和安全、自主和开放、管理和服务的关系，激发企业主动参与的内生动力。要在立法起草、政策出台、标准制定等方面为行业自律留下充分的空间，鼓励企业开展合规认证、安全自评等方面的工作探索。

创新政府监管手段方法。政府监管部门既要“查管罚”，又要“守疏戒”，加强重点领域关注和关键问题导向，可适当引入第三方认证、信用评价等方法。强化用户个人信息保护监测，建立面向保护态势、重点问题、行为规范等常态监测机制与技术能力，及时发现问题和解决问题，引导产业健康发展。

鼓励企业强化内部数据治理。要督促企业贯彻“隐私设计”理念，建构与风险程度相适的安全防护措施，采取进行经常性审计、合作伙

伴数据安全水平评估等方式，多措并举提升个人信息保护水平。这些措施既是着眼于安全保护的需求，也是优化个人信息使用的路径，能够鼓励企业从根本上树立个人信息及隐私风险意识，规范个人信息的收集、使用行为及安全防护。

完善多方协同参与机制。进一步完善政府、企业、行业组织、用户等多方协作、共同参与的个人信息保护机制，综合运用法律、监管、技术、市场、社会等手段，形成一套以法律法规和标准规范为基础，以政府监管为主要驱动，以行业自律和用户监督为重要手段的综合性保护模式。

（四）主动探索个人信息保护的新型技术

标识加密技术。以差分隐私、同态加密等为代表的加密技术，能够利用算法将个人信息中的标识信息转换成密文，在确保数据完整性的情况下实现个人信息顺利流通。在加密以后，还可以通过技术手段让不同的被加密标识通过第三方转译再次进行关联，从而确保流通中的关联性，保持数据使用价值。

追溯审计技术。通过建立针对个人信息全生命周期的追溯审计机制，能够及时发现个人信息泄露迹象。要对企业各部门和合作伙伴做到透明日志记录，让数据保护人员能够及时查阅并发现问题；要及时检测日志记录中的异常现象并快速定位，进行源头追溯。

区块链技术。区块链技术具有去中心化、信息可追溯等特点，可以塑造可信的数据使用环境。区块链通过使用链式数据结构进行验证

和存储，确保个人信息写入和读取的完整性；区块链具有公开透明的特征，能够让信息的使用过程不可篡改，防止个人信息被滥用；区块链可以通过共识机制确保数据交易的全网可验证，确保个人信息的完整性。

CAICT 中国信通院

CAICT 中国信通院

中国信息通信研究院

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-68032749、62304839

传真：010-62304980

网址：www.caict.ac.cn