我的信息我做主

大数据杀熟、不授权APP使用个人相关信息就无法使用或无法使用其全部服务、个人信息被售卖……随着互联网的飞速发展，消费者享受着互联网带来便利的同时，个人隐私泄露、个人信息被过度使用的事例近年来也比比皆是。

11月1日，《中华人民共和国个人信息保护法》（简称《个人信息保护法》）正式实施，该法明确不得过度收集个人信息、大数据杀熟，对人脸信息等敏感个人信息的处理作出规制，完善个人信息保护投诉、举报工作机制，为破解个人信息保护中的热点难点问题提供了强有力的法律保障。

随着《个人信息保护法》的实施，对网络生活有怎样的影响？对个人信息保护有哪些支持保障？平台隐私政策是否存在违规风险？信息保护与数据共享又该如何平衡？

个人信息保护长期成薄弱环节

“我已阅读并同意用户服务协议。”——网上有段子说，这是最大的“谎言”。

动辄万余字的冗长条款，夹杂着各种专业术语和法律名词，颜色浅字号小排版密，“让人一看就读不下去”……

能选择不同意吗？若“不同意”，就会被“一言不合玩闪退”。想要使用这款应用，必须“被迫同意”。

据一项调查发现，77.8%的用户在安装APP时“很少或从未”阅读过隐私协议，在被调查的150款APP中，近三成APP存在制造障碍、刻意隐藏和诱导用户略过隐私协议的行为，受访对象对于隐私协议的认可程度处于较低水平。被忽视的用户服务协议和隐私政策条款，常常会为违规或者过量收集个人信息大开方便之门。中国信息通信研究院泰尔实验室主任宁华介绍，从近年来出现的情况看，主要存在以下安全风险：

一方面，在用户不知情的情况下，过度收集和使用个人信息。“一些智能设备并未通过隐私政策或其他途径明确告知用户收集使用信息的目的、方式、范围和频次，也未向用户提供明确的允许和拒绝的选项。”宁华说，这种累积性的权益侵害如果出现在日常生活中，将引发用户担忧。

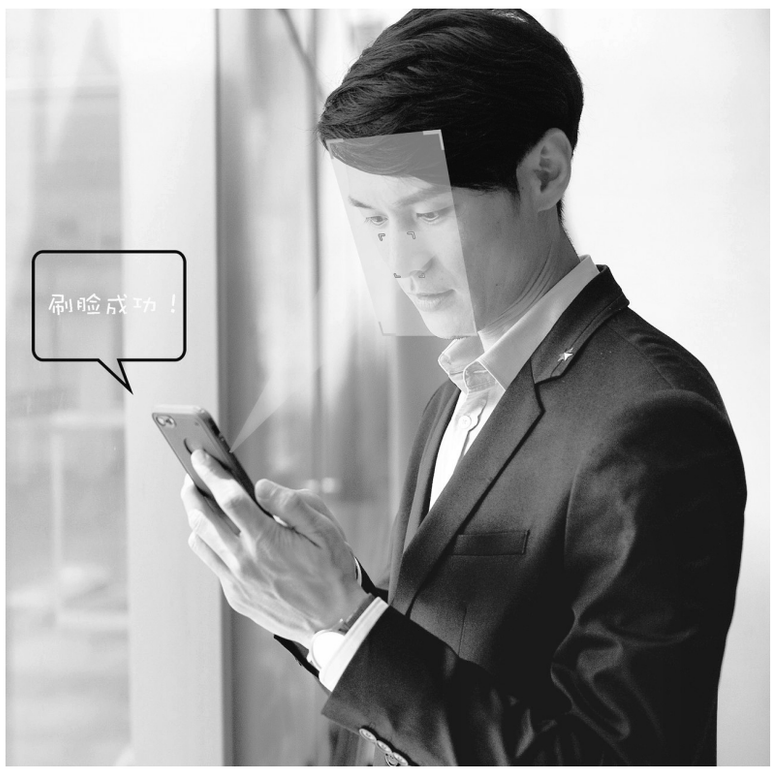
另一方面，在收集处理个人信息时，规则较为模糊。宁华提出，一些智能终端可同时接入更多设备，当用户和其中一款智能终端语音交互时，倘若在其隐私声明中，没有明示声纹、指纹等敏感信息存储、转移和二次加工等方面的妥善处理方式，一旦数据泄露，会造成广泛的恶劣影响。

“个人信息的保护长期以来是个薄弱环节，同时又是一个涉及14亿多人民群众的大工程，靠政府、靠机构保护是不够的，更多的是让每个公民举起法律武器，保护好个人的有关信息。”全国人大常委会委员乌日图表示，要大力推动法律的宣传，使大家充分认识到个人在信息保护方面的权利和义务。

“个人要提升个人信息保护素养，不要轻易把自己的个人信息交给那些来路不明的APP。”对外经贸大学数字经济与法律创新研究中心执行主任许可提醒，个人可以积极行使《个人信息保护法》规定的查阅权、复制权、更正权、删除权等一系列权利，及时了解、把握自己的个人信息收集和处理情况。

当前，随着《个人信息保护法》的实施，以上这种“产品方在假装很认真告知，用户在假装阅读并同意”的情况有望迎来重大改变。

“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”“个人有权撤回其同意”“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”……在规定“告知—同意”核心规则之时，《个人信息保护法》特别明确，个人信息处理者在处理个人信息前向个人告知相关事项时，“应当以显著方式、清晰易懂的语言”真实、准确、完整告知，处理包括人脸等在内的敏感个人信息时，必须取得单独同意。



遵循知情同意和最小必要原则

安装图像处理程序，要提供地理位置信息；下载文字编辑APP，需获取通讯录权限；在公共场所毫不知情时，人脸信息可能被记录……有人说，对于生活在信息化时代的人们，这是一个最好的时代，也是一个最坏的时代——

面对疫情防控形势，可以“一码走天下”，犯罪嫌疑人在联网人脸识别系统下无所遁形；但人们在享受数据带来便利的同时，也对信息收集处理的尺度、界限有着高度的敏感。

按照相关规定，APP收集处理用户信息应该遵循“收所必需、用所必需”的基本准则，所收集、处理的信息应该处于“必需”，且在合理的时间段、规定的业务范围内被正当使用。

《个人信息保护法》第16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。

“这里的‘必需’怎么认定？由谁来确定？这就很关键了。”全国人大常委会委员彭勃表示：“现在人民群众对于个人信息保护反映最大的，就是个人信息处理者过度采集和占有公民个人信息。某种意义上来讲，我们制定这个法恰恰就是为了约束这个。要对供应和服务运营商、信息处理者进行严格、科学的约束和规范。”

许可表示，这里的“必需”条款，源自个人信息处理的最小必要原则。“提供产品或服务所必需”，必须从用户和企业两方来看，不能只看单方面的企业观点，也不能只看单方面的用户观点，而是要通过双方的合意来判断。

根据《个人信息保护法》第26条规定，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。全国人大常委会委员李巍观察到，实践中一些社区、银行、商店并不是完全按照这个规定，“或者说是以假借维护公共安全为目的，设置很多人脸识别等生物识别手段”，他建议采取措施防止滥用和扩大图像采集、人脸识别等手段。

许可表示，“为维护公共安全所必需”应当遵循行政法上的比例原则。“为了维护公共安全而处理个人的敏感信息，特别是人脸信息，应当遵循其必要性。即是为了实现特定的公共目的之必要，不能超出维护公共安全目的。”

宁华分析，智能设备与用户紧密绑定，设备上的数据密切反映了用户的行为特征，叠加与之配套的APP交叉验证，呈现出较高的商业价值，不少商家铤而走险、违规使用。

“一些违规收集个人信息的行为存在技术复杂、隐匿性强、感知性弱等问题，难以追根溯源，再加上很多人个人信息保护意识不够，从而产生侵害用户权益的问题。”中国人民大学公共管理学院教授马亮说。

在马亮看来，种种侵害用户权益行为不仅使个人信息面临过度采集、滥用等问题，增加了因信息泄露而危害人身财产安全的社会风险。从长远看，还将影响消费者对移动互联网等应用场景的信任，使数字经济发展面临挑战。

应该看到，近年来随着用户权益保护意识不断增强，对智能设备的治理网络也在越织越密。

2013年4月，工信部印发《规范互联网信息服务市场秩序若干规定》，明确提出生产企业不得在移动智能终端中预置未向用户明示并经用户同意，擅自收集、修改用户个人信息的应用软件；2016年12月，《移动智能终端应用软件预置和分发管理暂行规定》出台，再次明确未经明示且经用户同意，不得实施收集使用用户个人信息、开启应用软件等侵害用户合法权益或危害网络安全的行为。

今年5月以来，中央网信办会同工信部、公安部、市场监管总局推进摄像头偷窥等黑产集中治理工作，对非法利用摄像头偷窥个人隐私画面、交易隐私视频、传授偷窥偷拍技术等侵害公民个人隐私行为进行集中治理。

针对智能网联汽车的网络安全问题，前不久，国家网信办、国家发改委、工信部等五部门发布《汽车数据安全管理若干规定（试行）》，明确提出利用互联网等信息网络开展汽车数据处理活动，应当落实网络安全等级保护等制度，加强汽车数据保护，依法履行数据安全义务。

“一系列法律法规明晰了智能设备等终端生产企业和互联网信息服务提供者的信息处理行为应遵循‘知情同意’和‘最小必要’两项个人信息保护基本原则。”宁华说，与此同时，智能设备系列行业标准结合具体应用场景，细化了“知情同意”“最小必要”的认定标准，进一步廓清了信息收集正当与不正当、适当与过度之间的边界。

信息使用在法律中明确界限

“之前在市里分别打车，相同的起点和终点，因为手机型号不同，车费就不一样。”“我和朋友在同一时段购买相同品牌的衣服，由于朋友经常网购比较贵的商品，结果他没有收到优惠信息，价格比我高出几十元。”通讯录、相册、摄像头、麦克风……如今下载运行一个APP，要多次点击“同意”“允许”。

移动互联网方便了生活，但个人信息却暴露无遗。

针对上述问题，我国曾相继出台《信息安全技术个人信息安全规范》和《网络安全实践指南——移动互联网应用基本业务功能必要信息规范》等文件，对APP超范围收集、强制授权、过度索权等个人信息安全问题作了明确规定，国家网信办、工信部等部门也多次公开过度收集个人信息APP名单并责令整改。不过，众多产品轻视法规、打擦边球等情况仍广泛存在。

目前，《个人信息保护法》作出了严格的限定。如第24条规定直指大数据“杀熟”：“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。”

此外，《个人信息保护法》第58条还规定，提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应成立主要由外部成员组成的独立机构对个人信息保护情况进行监督。

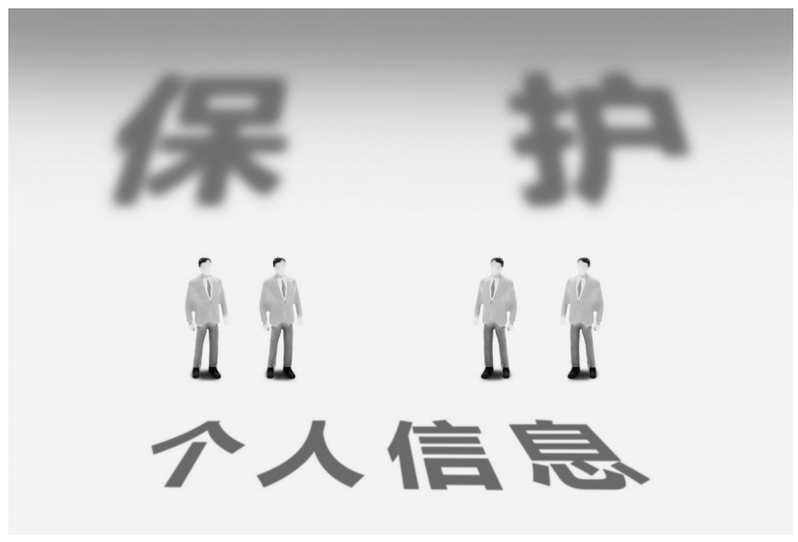
此外，法律还加强了对包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹在内的敏感信息保护，并为不满14周岁未成年人信息制定专门的个人信息处理规则，相关条款对过去个人信息保护实践中存在问题的领域进行了重点回应。

“现在是既怕贼偷又怕贼惦记。我们很多信息和秘密都存在手机里，这么多应用却能想看就看，感觉很没有安全感。”北京石景山的李女士最近刚换了新手机，她的担忧将随着《个人信息保护法》的实施迎来转机。

处理个人信息应当“遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息”“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”；收集个人信息应当“限于实现处理目的的最小范围，不得过度收集个人信息”“遵循公开、透明原则，公开个人信息处理规则”……在对应用程序收集、处理个人信息行为作出明确规范之外，《个人信息保护法》还规定了违法行为惩处规则，对违法处理个人信息的应用程序，最高可处5000万元罚款。

“随着个人信息保护法的施行，相关执法有了更加明确的法律依据。”北京大学法学院教授薛军表示。

信息保护与数据共享如何平衡？



德恒上海律师事务所合伙人高亚平表示，《个人信息保护法》中的一个重要原则就是阐明谁在采集你的信息以及将作何用途。“我觉得我用APP的时候就很紧张，到底谁在收集我的信息？”

《个人信息保护法》高达5%营业额的史上最严罚则给不少互联网平台敲响了警钟，平台纷纷调整更新其平台隐私政策。然而，当高亚平团队细细阅读平台调整后的隐私政策时，却发现不少平台在隐私政策使用主体上暗藏玄机。

“理论上大家普遍默认信息收集的主体是主导APP的某一家公司，但实际上许多平台都在各自隐私政策中宽泛地解释信息收集主体为‘我们’，这与《个人信息保护法》完全冲突。你去看它的隐私政策，它（信息收集主体）会被无限放大，它通常被定义为一个集团公司，同时包括了它的关联公司，甚至是它未来可能增加的关联公司。”虽然存在上述极端情况，但高亚平也指出，合规的平台也是存在的，并且大平台都在为《个人信息保护法》的实施做准备，优化隐私政策，但仍有很长的路要走。

高亚平补充说，《个人信息保护法》具体的法条中，违法情节严重的主体或处上一年度营业额百分之五以下的罚款。目前“情节严重”并无明确的定义，处罚边界模糊，平台一旦将信息收集主体宽泛化，最终处罚主体也很有可能包括整个集团。因此，在高亚平看来，平台一味将信息收集主体扩大，最终可能是“搬起石头砸自己的脚”。

高亚平认为，平台调整隐私政策或授权协议短期内会提高平台的合规成本，但从长期来看，避免了劣币驱逐良币现象的出现，整个互联网生态将得到优化。“整个交易成本的确提高了，但是它的商业机会更多了。”

高亚平团队根据既往的个人信息保护合规的项目经验，提炼《个人信息保护法》中个人信息处理者的法定义务，总结出“MAC-TOP”合规“武器”，用于判断某互联网平台是否做到个人信息保护合规，在《个人信息保护法》规定的举证责任倒置原则下，面对投诉或纠纷时，平台能否“自证清白”。

中南财经政法大学数字经济研究院执行院长、教授盘和林表示，数字经济本质上是利用大数据挖掘市场需求，从而引导产品服务规划，满足各种差异化需求，动态促进市场供需平衡。因此，合理利用和挖掘数据价值是进一步发挥数字经济优势的关键所在。

盘和林说，良好的信息保护是数据共享的基本前提，《个人信息保护法》的出台和落地，从法律层面彰显了国家对信息保护的重视和决心，原先被诟病的大数据“杀熟”、数据外泄和被非法利用等问题，在很大程度上会得到遏制和改善。但他担心，法律开始实施之后会出现数据过度保护的问题。

他认为，《个人信息保护法》的初衷是在保护好个人信息的前提下，促进数据要素的流动利用。为了保证社会效益和经济效益最大化，保证数字经济健康有序发展，法律在运行过程中也需要进行权衡。“这个度的拿捏实际上有待于我们在法律实施之后，在一段时间内来进行观察。”

面对《个人信息保护法》的落地，盘和林也建议，平台应有简易透明的隐私保护规则和完备的信息保护机制，同时保证必要的技术能力为用户信息提供保护，并接受信息监管部门的监管，站在消费者的角度认认真真地履行法律。

本文综合自光明日报、央广网、人民日报、中国水运网等媒体报道