Dispute Settlement 争议解决, 2023, 9(6), 2680-2690
Published Online November 2023 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2023.96366

APP侵犯个人信息的实证研究

贾金月

上海政法学院刑事司法学院，上海

收稿日期：2023年9月22日；录用日期：2023年10月26日；发布日期：2023年11月3日

摘　要

随着网络的发展，“应用为王”的理念已经深入人心，这意味着网络上的各种应用将会给你提供更多的信息，更多的服务，更多的娱乐。另外，随着技术的不断发展，这些应用程序的功能也越来越丰富，它们可以在不知不觉中收集到使用者的个人资料，然后再经由网络传送出去。随着网络游戏实名制、社交软件、电子商务等各种形态的兴起，也造成了使用者将更多的真实信息曝光在互联网上，从而对使用者的隐私造成了严重的威胁。众多学者在此方面的研究更多的是采用的定性研究，很少采用定量研究。本文借助SPSS软件，结合中国裁判文书网和北大法宝案例库中的司法实践案例以及相关的资料和数据的基础上，对APP侵犯个人信息案件进行梳理，并找出目前此类案件的一些现实困境和问题。

关键词

应用程序，个人信息，现状，困境

An Empirical Study on APP Infringement of Personal Information

Jinyue Jia

School of Criminal Justice, Shanghai University of Political Science and Law, Shanghai

Received: Sep. 22nd, 2023; accepted: Oct. 26th, 2023; published: Nov. 3rd, 2023

Abstract

With the development of the Internet, the concept of “application is king” has been deeply rooted in people’s hearts, which means that various applications on the Internet will provide you with more information, more services and more entertainment. In addition, as technology continues to evolve, these applications are becoming more and more versatile, allowing them to unknowingly collect personal data from users and then transmit it over the network. With the rise of online game real-name system, social software, e-commerce and other forms, it also causes users to ex-

文章引用: 贾金月. APP 侵犯个人信息的实证研究[J]. 争议解决, 2023, 9(6): 2680-2690.
DOI: 10.12677/ds.2023.96366

pose more real information on the Internet, which poses a serious threat to users' privacy. Many scholars in this area of research are more qualitative research, and few do quantitative research. This paper, with the help of SPSS software, combined with the judicial practice cases in China Judgment Documents Network and Peking University Magic Talisman case database as well as relevant materials and data, sorted out the cases of APP infringement of personal information, and found out some realistic difficulties and problems in such cases.

Keywords

Application Program, Personal Information, Current Situation, Dilemma

1. 引言

截至 2022 年 12 月，较 2021 年 12 月增长 3549 万，较 2021 年 12 月提升 2.6 个百分点。中国的用户数量快速增长，网络的基础建设日趋健全，并且随着用户数量的增加，我国网民规模达 10.67 亿，而互联网普及率达 75.6%。值得注意的是，目前我国手机网民规模达 10.65 亿，以移动电话为主要网络访问方式的网络用户已上升到 99.8%。[1] 移动用户更多的是使用了大量的信息获得和通信交流的软件。移动网络的迅速发展是推动我国移动用户数量迅速增加的主要因素之一。随着 5G 应用的持续推广，以 5G 为基础的移动互联网业务变得更加丰富，搜索引擎、短视频、网络游戏、即时通讯、第三方支付平台(支付宝、微信等)、C2C 电子商务平台(京东、淘宝、天猫等)、生活服务电子商务平台(美团、大众点评等)等等，这些应用都在飞速发展，从而吸引了更多的手机网民。

从 2006 年“虐猫事件”使人肉搜索一词进入大众事业引发了网络上的争论，而 2008 年的“艳照门”事件以及后续各种“门事件”的曝光，再到近期的蔚来汽车用户数据遭大量泄露等等，让人们对网络上的个人信息产生了更深层次的理解。随着时间的推移，一系列新的网络争议——互联网首例应用软件侵犯用户隐私权纠纷“3Q 大战”[2]、Facebook 的“隐私门”[3] 等揭示了网络产业发展面临的另一新问题——网络应用收集用户数据，侵害了用户的个人信息，给 APP 用户的隐私权带来新的威胁。在这些事件中，这几款应用程序都被指责为非法收集和发送用户信息，但大部分问题都仅限于非正式的一些报道，并没有形成一个具有权威性的结论，对于这些应用软件到底是不是侵害了用户的隐私，也没有明确的定性。但在不久前，工信部组织第三方检测机构对群众关注的生活服务类移动互联网应用程序(APP)及第三方软件开发工具包(SDK)进行检查。发现 46 款 APP (SDK)存在侵害用户权益行为，其中涉及的教育类 APP 共 7 款，包括小初高同步课堂、星火英语、懒人驾考、同桌 100、贝聊家长版以及宝宝巴士品牌旗下两款产

[1] 第 50 次<中国互联网络发展状况统计报告>》https://www.cnnic.org.cn/n4/2022/0914/c88-10226.html, (访问日期：2023 年 6 月 5 日)。
[2] 2010 年 10 月 28 日，360 公司在北京宣布，通过微软的 Process Monitor 和 360 隐私保护器，发现了中国第一大客户端软件 QQ 在扫描用户硬盘时出现极其异常的行为。用户登录 10 分钟后，QQ 软件即开始按照一个预置的“超级黑名单”扫描电脑开始菜单和桌面上的快捷方式。微软 Process Monitor 和 360 隐私保护器都显示，这个名单里共包含 685 款软件，用户能接触到的几乎所有互联网软件都纳入其中。
[3] 2010 的 10 月 19 日，《华尔街日报》上有消息报道，多个 Facebook 上最热门的应用程序会将用户的个人资料分享给广告商和网络追踪公司，违反了 Facebook 的隐私规定。报导称，应用程序让至少 25 家广告和数据公司可以访问使用者的名字，在某些情况下来可以访问使用者的朋友名字。这个问题可能影响到数千万的使用者。前十大最热门的应用程序，包括 Zynga 的 Farmville 都会把使用者的 ID 发送给第三方厂商。这暴露了 Facebook 要面对的保护用户隐私的挑战。

品。上述 APP 被通报所涉问题多为违规或超范围收集个人信息，违规互联网弹窗信息推送服务、APP 强制、频繁、过度索取权限等。

从 QQ 与 360 的对峙到 360 的信息泄露事件，网络应用对用户个人信息的侵害正在逐步变得清晰起来，从最初的猜疑变成了确切的事实，从简单的浏览用户的电脑屏幕上的快捷键到泄露用户的访问信息、注册信息和购物信息，冲突越来越激烈。在网络战争中，该怎样保障用户的隐私？在互联网的背景下，对个人隐私权的保护已是当务之急，下面将对如何对网络中涉及的用户个人信息进行探讨。

2. 个人信息概述

(一) 个人信息概念

“个人信息”又称“个人资料”、“个人数据”。目前，国内已经对个人信息进行明确的立法，2021 年 8 月 20 日，《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》)经十三届全国人大常委会第三十次会议表决通过，自 2021 年 11 月 1 日起施行。《个人信息保护法》第四条对公民个人信息进行了界定，将公民个人信息界定为：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。

个人信息一种独立的纯粹的人格法益是指各类信息，用以显示和标识自然人的信息，通过对信息的分析、挖掘和智能关联，可以构成一个“数字人格”，而这个“数字人格”既可以反映出一个人的人格，又可以作为一个个体的一种表达方式，同时还可以作为一个个体对自己的认识。[1]

(二) APP 相关概述

软件可分成两类：一类是系统软件，另一类是应用软件。APP 其实是 APPlication Software (应用程序或者说应用程序)的简称。伴随着互联网的发展，APP 的类型越来越多，其功能越来越强大，能够为使用者带来越来越多的综合性体验和便利。除此之外，伴随着智能手机的持续更新和升级，APP 的移动客户端也在持续发展，5G 时代的来临，使得移动应用软件的发展进入了一个迅速扩张时期。

虽然网络上的各种应用程序给人们带来了很多方便，但同时也存在获取用户个人信息的问题。其中有两种主要类型：

1) 手机应用软件搜集个人信息

Facebook 的例子让我们看到了另外一个可怕的问题，那就是，我们的手机上应用程序能做到的事情比我们想象的要多。因此随着智能电话和各种应用软件的普及，人们对个人信息的泄露问题也越来越感到头痛。这一新型的面向客户的业务模式具有巨大的利润空间，但是如果不能有效地控制和利用这一模式，就很难实现其最大的价值，消费者也将远离它。此外，这些应用程序还会从用户的手机中收集相关的数据，并将这些数据发送到应用程序开发商中。例如，某些应用软件下载更新服务平台，通常被称作“应用商店”，它会收集在用户手机中已经安装过的某些应用软件的信息，并将这些应用软件的独特包名发给开发者后台，后台就可以利用这些数据来增加和更新自己数据库中的应用软件，从而促进自己的发展。当一个应用程序被安装好之后，它就会告诉你它所要用到的权限。比如，假如有一个应用软件，它需要查看手机系统的通话记录，那么它会在安装的时候给使用者一条信息，信息大致如下：“程序运行过程中需要查看您的通话记录”，同时也会给出同意或者不同意的选项，但多数情况下只能选择同意选项，因为只有同意才能继续安装，如果选择不同意将退出安装。若“同意”，此应用程序就有查看电话呼叫的权利，并顺利地进行了安装，若使用者点击“不同意”，此应用程式就不能进行安装。从技术角度来说，应用软件要获取某种权限，在编码的时候，就只需在代码中写入需要申请的 Root 权限，当应用程序运行的时候，就会执行向用户申请权限的动作。root 权限，系统权限的一种，也叫根权限。在 Linux 系统中，root 用户具有系统中所有的权限，如启动或停止一个进程，删除或增加用户，增加或

者禁用硬件等等。因此，Android 系统中 root 也具备最高级别的管理权限，可访问和修改系统中几乎所有的文件。[2]

2) 个人计算机上的应用软件搜集用户电脑里的信息

从 3Q 大战到 360 个人信息泄露事件，很多安装在个人计算机上的网络应用，都能够检测到用户的使用数据，包括他们的账号信息、访问记录等等并予以收集。其中包含：a) 所采集的使用者账户资料；b) 对使用者进行 24 小时的监控，并对使用者的一切访问行为进行纪录；c) 对使用者的检索项目进行登记；保存企业内部网络的重要资讯。Windows 是常用的电脑操作系统，Root 是一个高级 Administrator。普通用户所接触到的是 Windows nt 内核系统，在 Windows nt 内核系统中，当用户在安装一个应用软件之后，该应用软件的权限会被默认为用户的权限，假如用户是 administrator，那么就会执行 administrator 的权限。[3]这就为应用程序对电脑用户进行收集带来了很大的方便，简而言之，就是可以对应用程序中的用户所能查看的数据进行搜索和收集。在用户安装一款 APP 时，通常不会想到该 APP 会在自己的意志以外，根据 APP 开发者的意志进行其它的操作，所以在 Windows nt 系统下，网络应用软件想要收集用户信息就比较容易了。

通过对应用程序搜集用户信息行为的剖析，我们可以归纳出其目的如下：

a) 构建平台。有些网络软件开发者，在研发的早期，他们在构建数据库的时候，会消耗很多的资源。如果他们要在发展的早期，在很短的时间里构建出自己的数据库，并将其整合到用户喜爱的应用软件上，就必须对用户的电脑或者手机上的已安装的应用程序进行收集，这样才能为用户提供更多的服务，从而提高他们的竞争力和影响力。b) 满足用户需求。网络产业同样只有抓住了用户的需求，商机才会出现。收集用户安装的应用情况，分析出哪些类型的应用软件拥有较大的用户基础，从而向这方面延伸或发展。c) 恶意竞争。利用收集在用户电脑上的竞争对手的信息，从而实现了一种恶意竞争。一般地，采用这种方式进行恶意竞争的企业，会对其对手的用户基数，还有竞争对手的装机量等能够反映其发展状态的数据产生了浓厚的兴趣。d) 精准化。网络应用程序的最大竞争是对使用者喜好的掌握和对使用者需要的集成。精准营销以精确地获得使用者的个人资料为先决条件，因此，如何保障使用者的隐私权已引起了全社会的高度重视。精准指的是利用技术手段，对用户的行为和信息进行分析，在海量的数据的基础上，得出相对的准确度。

3. APP 侵犯个人信息现状

(一) 选材与数据

要想对我国侵犯个人信息的现状进行深入的调查，就必须对当前的司法状况展开数据的分析，从司法实践中发现当前我国所面临的问题，从而为接下来对相关的问题进行的分析和讨论提供一个可靠的现实依据。为了更好地了解近几年的司法判决情况，案例库的选择也是非常重要的。虽然中国裁判文书网案例丰富，相较于其他数据库和网站更权威性，更具代表性，但是如果案例过多则只能检索前 600 条案例，因此本文选择的案例库是以北大法宝的案例库为主。因为最高人民法院印发《关于修改〈民事案件案由规定〉的决定》的通知将“6.隐私权纠纷”案由变更为“8.隐私权、个人信息保护纠纷”案由。这使得本文作者于 2023 年 5 月 30 号在北大法宝“案由”中，依次选择“民事”、“人格权纠纷”、“隐私权、个人信息保护纠纷”“个人信息保护纠纷”，发现只有近两三年的个人信息纠纷案件，也就是说在 2020 年之前个人信息纠纷和隐私权纠纷是放在相同案由中。因此，笔者是以“案由：隐私权、个人信息保护纠纷；专题分类：个人信息保护纠纷；文书类型：判决书”为检索条件进行检索，共计检索到 621 件判决书。因为裁定书等文书可能不包含案件事实所以是排除在外的。我们对个人侵权案件整体检视发现(见图 1、图 2)：

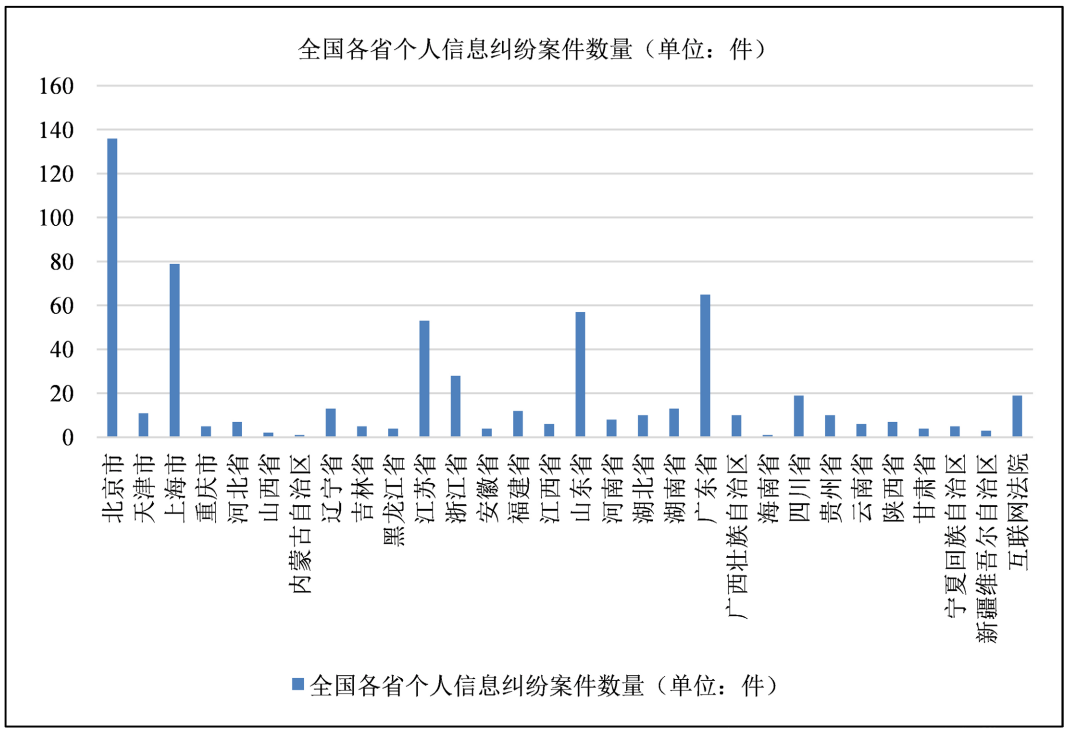

Figure 1. The number of personal information dispute cases in each province
图 1. 全国各省个人信息纠纷案件数量

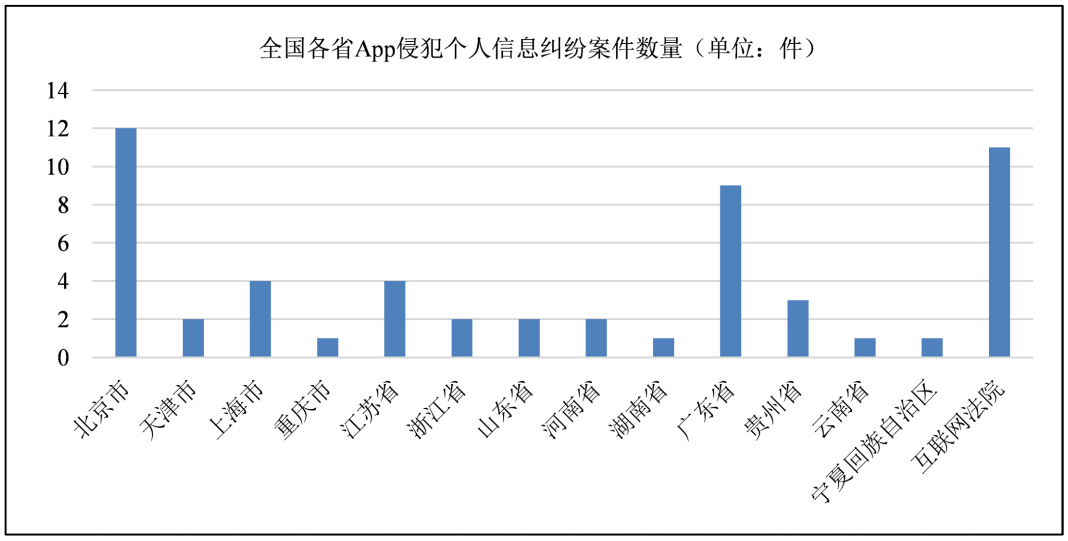

Figure 2. Number of disputes involving APP infringement of personal information in various provinces
图 2. 全国各省 APP 侵犯个人信息纠纷案件数量

通过对 621 件案例进行分析，发现北京、上海、广东、江苏、浙江和山东的案例都是比较多的。六个省的病例总数，在全国案例总数中所占比重有将近七成。从地理位置来看，除了北京之外，这六个省份都是珠三角和长三角这两个发达的省份，从这一点来看，在具有较高的经济活力的省份，个人侵权案件的发生率是比较高的，其居民的法治意识也比较高，在权利遭到侵犯之后，会选择采取法律手段有更多的诉讼活动。

(二) 样本案例的统计情况

1) 样本案件胜诉情况(见表 1)

对样本案例的胜诉情况进行统计，发现在有效的 36 个案例中，胜诉的比例并不算高，仅有 18 件，占比 50%，与败诉的比例是一样高的，在与 APP 背后的公司诉讼过程中，原本就出于弱势地位的个人从诉讼的结果来看更显被动。

Table 1. Table of successful cases of sample cases
表 1. 样本案件胜诉情况表

判决结果					
		频率	百分比	有效百分比	累积百分比
有效	胜诉	18	50.0	50.0	50.0
	败诉	18	50.0	50.0	100.0
	合计	36	100.0	100.0	

2) 原告诉求的支持情况

通过对样本案件中原告主张的支持进行了统计，得出了如下(见表 2)结果：其中仅有一件案件中的原告的诉讼请求得到法院全部支持，仅有占比仅有 5.6%；18 件案件中，原告的要求获得了部分的支持，约为 94.4%。这主要是因为在笔者研读案例的过程中发现不少原告在起诉的过程中都主张财产损害赔偿以及精神损害赔偿，但从胜诉的案件中来看，两者得到法院支持的占比是比较低的(见表 3、表 4)。这里的财产损害赔偿是不包含诉支出费用的，财产损害赔偿占比 22.2%，精神损害赔偿占比也是 22.2%，这还是将败诉的情况排除在外的。

Table 2. Support for the plaintiff's claim
表 2. 原告诉求的支持情况表

原告诉求的支持情况					
		频率	百分比	有效百分比	累积百分比
有效	全部支持	1	5.6	5.6	5.6
	部分支持	17	94.4	94.4	100.0
	合计	18	100.0	100.0	

Table 3. Information on compensation for property damage
表 3. 财产损失赔偿情况表

是否存在财产损失赔偿					
		频率	百分比	有效百分比	累积百分比
有效	是	4	22.2	22.2	22.2
	否	14	77.8	77.8	100.0
	合计	18	100.0	100.0	

Table 4. Information on compensation for mental damage
表 4. 精神损害赔偿情况表

是否存在精神损害赔偿					
		频率	百分比	有效百分比	累积百分比
有效	是	2	11.1	11.1	11.1
	否	16	88.9	88.9	100.0
	合计	18	100.0	100.0	

3) 原告败诉的原因

通过对样本案件的分析，发现在样本案件中，原告败诉主要分为两种情形，见表 5。一种是在举证方面，原告在举证方面存在困难，在此情形下也存在两种情况，一是原告自身难以证明自己受到个人信息侵权，此种情况占比 23.5%，共计有 4 件。二是原告确实受到侵害，被告也确实存在着个人信息的处理行为，但是难以证明这侵害是被告的行为导致的，此种情况在所有案件中所占比例为 35.3%。还有一种是在法院审理过程中发现，被告在主观上并未存在过错，造成原告的误解，此类案件占比 41.2%。

Table 5. The cause of the plaintiff's loss
表 5. 原告败诉的原因情况表

原告败诉的原因					
		频率	百分比	有效百分比	累积百分比
有效	难以证明自己受到侵害	4	23.5	23.5	23.5
	被告主观没有过错	7	41.2	41.2	64.7
	难以证明因果关系	6	35.3	35.3	100.0
	合计	17	100.0	100.0	

4) 被告人承担责任的方式

一般情况下，法院会判定被告侵犯了原告的个人信息权益，会判决被告对原告进行赔礼道歉，并且会让其停止侵犯行为，但是很少支持原告要求的精神损害赔偿，对被告的承担责任方式展开统计，得出的结果(见表 6)：其中，36 件案件中，比例最高的是要求被告人承担多项责任，达 44.4%，这其中大多都包含赔礼道歉以及承担诉讼支出的费用，但主要费用主要是诉讼费用和公证费用。支持精神损害赔偿的共计有四件，但其中只有一件是以精神损害赔偿作为主要的赔偿方式。

Table 6. Table of modalities of accountability reported
表 6. 被告的责任承担方式情况表

被告的责任承担方式					
		频率	百分比	有效百分比	累积百分比
有效	赔礼道歉	5	27.8	27.8	27.8
	精神损害赔偿	1	5.6	5.6	33.3

Continued

诉讼支出费用	3	16.7	16.7	50.0
消除影响、恢复名誉	1	5.6	5.6	55.6
承担多项责任	8	44.4	44.4	100.0
合计	18	100.0	100.0	

5) APP 侵害个人信息的具体方式(见表 7)

从表 7 中可以看出，APP 泄露个人信息的情况是最多的，占比为 41.7%，除此以外还有以下几种侵犯个人信息的方式：

Table 7. Pattern of infringement
表 7. 侵权方式情况表

侵权方式					
		频率	百分比	有效百分比	累积百分比
有效	自动授权获取个人信息	5	13.9	13.9	13.9
	隐私协议设置默认同意	1	2.8	2.8	16.7
	应用程序服务或功能捆绑	2	5.6	5.6	22.2
	隐私协议设置“霸王条款”	6	16.7	16.7	38.9
	侵犯用户个人信息知情权	3	8.3	8.3	47.2
	APP 泄露个人信息	15	41.7	41.7	88.9
	电话、短信等方式侵扰他人的私人生活安宁	4	11.1	11.1	100.0
	合计	36	100.0	100.0	

a) 自动授权获取个人信息

如今，手机应用程序成为了侵犯个人信息的重灾区，也就是因为大数据在现在以及将来都可以产生巨大的经济效益，这也导致了某些开发者将目标转移到了个人信息的采集上。所以，在开发手机 APP 的时候，就会设定可以利用 APP 使用者的手机权限来对其所需的信息进行采集。按照法律和有关制度的要求，APP 想要获得个人信息，需要征得使用者的同意。然而，很多运营商为了达到自己的目的，过度采集和使用个人信息已经变成了一种常态。许多的手机 APP 在安装过程中都会在没有得到用户的允许的前提下，会自动收集个人信息，或者是在获得部分授权后，却获取授权之外的信息。在上文中论述过，在安装 APP 过程中，一般都会出现一个对话框，询问用户关于某些权限是否许可。然而，由于安卓的系统对某些 APP 的性质是开放性的，也就是说，当他们通过安卓的方式来安装某些 APP 的时候，这些 APP 无需进行任何的身份验证，就能直接得到取得系统的底层权限，如果他们没有手动的将这些权限限制或者关闭，那么他们的隐私信息将会的运营商窃取，许多时候，即便用户的信息已经被泄漏，他们也不会立即被察觉。所以，对于这些非法的 APP，政府已经采取了严厉的措施来进行整改，以更好更有效的方式来控制应用程序获取用户的个人信息。有下表可以看到在司法实践中，自动获取个人信息的占比约为 14%。

b) 隐私协议设置默认同意

从现行的法律规定来看，“默认同意”确实侵犯了 APP 用户的隐私，然而“默认同意”并不少见，每个人在使用 APP 的时候，都会受到“默认同意”的影响，尤其是通过浏览器而不是在应用商店中下载的 APP。从上表中可以看出，隐私协议默认同意的案件只有一件，但我们在日常生活中仍然应该保持警惕，要用大概率思维来应对。有些 APP 的隐私政策往往会在登陆界面上显示，而这些条款很容易会被忽略掉，这其中一方面是由于用户对 APP 的安全性认识不足，另一方面也是由于 APP 运营商没有“明示同意”选项。大部分的使用者都是不知情时接受 APP 所设定的条款，这也容易导致使用者的个人资料外泄，一些不良 APP 经营者将使用者的资料推送给第三方组织也是时有发生。为此，我们必须按照“明示同意”的要求，通过“自愿选择”的方式，让使用者以“明示同意”的方式表达自己的意愿，从而实现保护最大化.从我们收集对的数据来看默认同意的现象也是确实存在的。

c) 应用程序服务或功能捆绑致使权限同意捆绑

在 APP 信息收集使用的主体中，除了 APP 的开发商和运营者之外，还存在着第三方机构，主要是是广告商和其他提供辅助功能的机构。因此，会出现应用程序服务或功能绑定，归根结底是这些开发商实际上也是一个利益共同体，他们有着清晰的分工，个人信息的共享多层次的获得利益，这些问题对公众的切身利益造成了很大的损害。从我们收集对的数据来看默认同意的现象也是确实存在的，占比为 5.6%。要使 APP 的服务和功能得到规范化，就需要对 APP 中的数据采集做出严格的限定，而第三方开发商希望获得用户的数据时，也需要得到使用者的“明示同意”，而且有关方面也有明确的要求。其一是第三方开发商直接与使用者签订的个人隐私权协定，以明确使用者的意愿，其二就是运营商在签订条款的过程中对第三方进行说明，并且与用户代签协议。在实际的操作过程中，不管是在前一种情形下，还是在后一种情形下，这些情形表面上看起来是合法地获得了用户的个人信息，实际上却为服务或功能绑定带来了机会，而用户仅仅能够享受到一次性的同意权利。

d) 关于“霸王条款”的隐私协定

笔者在上文中对霸王条款已经做了相关的论述，从上表中可以看出“霸王条款”也是除泄露信息之外侵权最多的方式，占比为 16.7%。近几年，APP 运营商在搜集用户数据时设定“霸王条款”的情况日益增多，有些 APP 的隐私协议甚至可以让用户即使看完也是大脑一片空白，完全不明白对方说的是什么意思，但又不能不答应，因为一旦不答应，APP 就无法再继续使用，没有任何讨价还价的可能，因此，许多用户只能在迫不得已的情况下按下了“同意”按钮，这种明明是“霸王条款”下的无奈选择，但实际上却成了 APP 肆无忌惮地窃取用户数据的借口，“霸王条款”的背后，就是 APP 运营商为了达到自己的目的，进行的一种网络技术欺凌，这种行为不但侵害了客户的合法权利，而且无视了国家的法律。因此，政府应该制定相应的规章制度，在“最少信息”原则的基础上，做出相应的规定。此外，应用程序的开发与运营也应对使用者的个人资料给予足够的重视，不得利用使用者的资料来谋取利益。

e) 侵犯用户个人信息知情权

法律赋予个人查阅复制权，规定个人信息主体有权复制其个人信息，与之相对的就是个人信息处理者应当提供正在处理的个人信息的副本，这种副本的形式应当包括纸质的，也包括电子化的，其应当是结构化的、通用的及可读的。[4]其目的是确保其对个人信息的知情权和保持应有的控制，避免因为非法收集、处理个人信息而致其人身财产权益遭受侵害。从实现查阅复制权的功能价值、保护个人合法权益的角度考虑，查阅复制权的客体不仅包含个人信息本身，还应当包括个人信息处理情况。信息处理者利用自动化决策方式进行个人信息处理活动，如收集、使用了具有个人特质的信息，个人信息处理者应当在第一次使用时，向个人提供便捷的拒绝方式。信息处理者事前通过隐私政策等取得个人概括性同意，

以及事后提供拒绝方式，可视为对个人知情同意权的保障，此时，信息处理者利用个人信息进行自动化决策具有合法性基础。信息处理者通过自动化决策方式进行信息推送，未向个人提供拒绝的方式或拒绝的方式完全不能达到便捷性要求的，使用户不能依据自己的真实意思表示进行拒绝，则个人信息处理者违反了法定义务，具有违法性，应认定侵害用户个人信息权益。[5]

f) 电话、短信等方式侵扰他人的私人生活安宁

自然人的个人信息受法律保护；除法律另有规定或者权利人明确同意外，任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人的个人信息，也不得以电话、短信、即时通信工具等方式侵扰他人的私人生活安宁。从上表可以看到，通过这种方式侵犯个人信息的现象也是存在的。服务提供者通过收集到的自身产品用户的个人信息来向其推送其他服务，甚至相关的短信推送无法关闭或者退订。

4. 解决 APP 侵犯个人信息的对应措施

大家一方面享受着互联网给我们带来的便利和好处；但另一方面，个人信息随着手机，飘散到四面八方。如果个人信息不能得到很好保护，手机就变成了“手雷”——随时会炸响，给我们带来危险。这个问题大家讨论已久，焦虑已久。《个人信息保护法》开始实施后，包括过度收集个人信息、滥用人脸识别、大数据“杀熟”、个人敏感信息等等方面，法律都开始有了明文保护与制约。在解决 APP 侵犯个人信息这一问题上，国家有关个人信息监管部门、手机 APP 开发者和运营商都需要作出改变。

1) 建立健全个人信息监管机制，形成更专业化的管理

根据我国《个保法》第六十条的有关规定，在中央由国家网信部门在个人信息保护和监督管理工作中负责统筹协调，国务院有关部门在各自职责范围内负责；在地方，设置县级以上地方人民政府有关部门作为基层个人信息监管部门。[6]据此来看，我国还是设有专门的个人信息保护机构，针对自动授权获取个人信息的行为，个人信息保护机构应该依据《个保法》采取了严厉的措施来进行整改，以更好更有效的方式来控制应用程序获取用户的个人信息。

2) 明确手机 APP 开发者、运营商的义务

a) 明示“知情–同意”义务

《个保法》明确了个人信息处理活动应遵循的原则，构建以“告知–同意”为核心的个人信息处理规则，是保障个人对其个人信息处理知情权和决定权的重要手段。个人信息保护法要求处理个人信息，应当在事先充分告知的前提下取得个人同意，个人信息处理的重要事项发生变更的应当重新向个人告知并取得同意。而我国目前手机 APP 用户个人信息处理者通常采取的是“隐私协议设置默认同意”，不足以保障“知情–同意”机制的实现。因此手机 APP 开发者、运营商不要采取默认同意的格式，要明确告知 APP 用户，使用户对自己的个人信息处理有一个正确的认知。

b) 遵守“不过度索取信息”的义务

APP 开发商运营商经常设置“霸王条款”随意获取用户的个人信息，而根据《常见类型移动互联网应用程序必要个人信息范围规定》规定，APP 只可以获取其运营必要的个人信息。必要个人信息是指保障 APP 基本功能服务正常运行所必需的个人信息，缺少该信息，APP 即无法实现基本功能服务。如即时通信类的必要个人信息包括注册用户移动电话号码以及账号等；网上购物类的必要个人信息包括注册用户移动电话号码、地址、支付金额等。APP 的开发商应该遵守自己的义务，不过度索取用户信息。

c) 加快 APP 更新升级，设置合理的获取个人信息范围

科技时代的个人信息安全绝不能缺位，APP 开发者应该尽快调整相应功能设置与必要个人信息收集范围，跟上目前管理的节奏。APP 开发者应该设定收集个人信息的底线，更好地保护个人信息，促进 APP 市场健康发展。

参考文献

[1] 王利明. 论个人信息权的法律保护——以个人信息权与隐私权的界分为中心[J]. 现代法学, 2013, 35(4): 62-72.

[2] 邢晓燕, 金洪颖, 田敏. Android 系统 Root 权限获取与检测[J]. 软件, 2013, 34(12): 208-210.

[3] 何钰娟. 互联网应用软件搜集用户信息侵犯用户隐私问题研究[D]: [硕士学位论文]. 北京: 北京邮电大学, 2011.

[4] 程啸. 我国《民法典》个人信息保护制度的创新与发展[J]. 财经法学, 2020(4): 32-53.

[5] 杨立新, 赵鑫. 利用个人信息自动化决策的知情同意规则及保障——以个性化广告为视角解读《个人信息保护法》第 24 条规定[J]. 法律适用, 2021(10): 22-37.

[6] 招雅婷. 手机 APP 用户个人信息法律保护研究[D]: [硕士学位论文]. 济南: 山东财经大学, 2022.