

精准广告投放与个人信息保护研究

王天祎

北京外国语大学法学院, 北京

收稿日期: 2025年6月4日; 录用日期: 2025年6月16日; 发布日期: 2025年7月31日

摘要

大数据与算法推荐技术突破了时间与空间的重岩叠嶂, 也促进了精准广告投放的出现, 网络服务提供者与用户对个人信息的博弈也随之产生。本文通过界定精准广告投放行为的性质, 剖析其表层“精准”下的底层逻辑, 随后基于规范性分析及利益平衡视角论证精准投放行为的正当性与否。在对个人信息知情权与决定权以及信息控制权的检验中, 提出司法实践中应完善“告知-同意”制度及能少够用与必要原则的完善路径。规范行业自律、细化立法规制、治理互联网广告, 方能激励用户、网络服务提供者、广告主三者的多元共治, 实现数字法治。

关键词

精准广告, 个人信息权, “告知-同意”制度, 数字法治

Legal Study on Precision Advertising and the Protection of Personal Data

Tianyi Wang

Faculty of Law, Beijing Foreign Studies University, Beijing

Received: Jun. 4th, 2025; accepted: Jun. 16th, 2025; published: Jul. 31st, 2025

Abstract

Big data and algorithmic recommendation technologies have broken through the barriers of time and space, giving rise to precision advertising. This has consequently triggered a dynamic interplay between network service providers and users over personal information. This study begins by defining the legal nature of precision advertising practices, then delves into the underlying logic beneath its surface-level “precision”. Subsequently, it evaluates the legitimacy of such practices through normative analysis and a balancing-of-interests perspective. By examining the right to informed consent,

the right to data self-determination, and the right to information control, this paper proposes judicial refinements to the “notice-and-consent” framework, advocating stricter adherence to the principles of data minimization and necessity. To achieve digital governance under the rule of law, the study recommends: Strengthening industry self-regulation, Refining legislative oversight, and Enhancing internet advertising governance. These measures aim to foster multi-stakeholder co-governance among users, network service providers, and advertisers, balancing innovation with personal data protection.

Keywords

Precision Advertising, Right to Personal Information, “Notice-and-Consent” Framework, Digital Rule of Law

Copyright © 2025 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

大数据以其独有特征开启了一场重大的时代转型,引发了公众关于生活、思维与工作的重新思考[1]。壬寅年末,一场由语言处理机器人程序 ChatGPT 引发的人工智能风暴席卷学术界,致使人们从对元宇宙的幻想中剥离,转而回到对大数据与人工智能的讨论。打开手机,我们似乎早已被渗透得千疮百孔,APP 掌握着我们的身高、体重、住址、身份证号甚至各种密码。打开淘宝,它会知道我是一名体重偏大、消费水平有限、酷爱篮球的学生;打开抖音,第一条永远是近期关注的美食、宠物、搞笑视频;甚至打开地图,“家”和“学校”字样清晰标注着我的行动轨迹,打车总是需要 29.16……“个人信息”似乎成为资本挖掘的富矿,网络服务提供者不断地收集、使用,直至敛财。

数据的井喷使人变得“透明”,最直接的体现便是广告的投放。2022 年中国互联网广告数据报告显示,中国市场互联网广告总体收入自 2017 年开始急速狂飙,于 2021 年到达巅峰值 5435 亿元人民币,同比增长率却不断下跌,甚至在 2022 年出现七年来首次负增长。大数据技术与短视频平台崛起,带来海量数据红利与精准的广告设置,市场规模逐渐步入深水区,即意味着数据潜在的市场潜力几近榨干,消费群体不再信任“精准投放”骗局,也揭开个人信息保护与精准广告投放冲突的面纱。

号称“取之于民,用之于民”的网络服务提供者,对个人信息的蚕食属于什么性质?精准广告行为是否具有正当性?面临网络空间中的数据围城,我们又该如何“突围”?

相比于无差别的普通广告,精准广告与用户之间的相关性更为密切。因此,想要解决精准广告投放与个人信息保护两者间的冲突,应从精准广告行为的性质界定入手。

2. 精准广告投放行为性质界定

2.1. 精准广告的生产与投放的表层现象

大数据凭借高效的数据挖掘、分析、利用能力为精准投放广告做“背书”,从而为网络广告精准投放的实现提供了技术基础[2]。作为大数据在广告行业应用的新型成果,精准广告被定义为:“行为广告(Behavioral Advertising)是指通过分析用户设备(如电脑或手机)在特定时间段内的网络行为数据(包括网页浏览记录、在线服务及应用程序使用情况等),推断其个人偏好与兴趣,进而向其推送定制化广告的营销

方式。¹简言之,广告商基于大数据设定的筛选条件,锁定目标用户群体,设计针对性广告内容,实现精准化信息投放[3]。这种“窄广告”即精准广告。

从技术层面看,实时竞价(RTB)是实现精准广告的核心。其运作流程如下:当用户访问某一网页时,该网站会向广告交易平台(Ad Exchange)发送广告请求;随后,交易平台向接入的需求方平台(DSP)广播竞价邀约,例如“某网站当前有一位潜在用户,是否需要投放广告?”与此同时,DSP会调用大数据管理平台(DMP)的分析能力,对该用户的浏览历史、兴趣标签等行为数据进行实时评估,并据此完成广告品类匹配与动态竞价。这种“精准性”的本质在于:通过海量非特定用户的网络行为数据建模,预测个体偏好,进而实现“千人千面”的定制化广告推送[4]。这一特点的实质往往针对“人群”,而非“特定”的某一用户的个人信息。网络服务提供商利用数据挖掘技术,对用户的内容浏览记录、消费行为数据及社交网络关系等多元信息进行分析,通过聚类算法将具有相似特征的人群归类(即“标签化”)。这种基于大数据的用户画像技术能够深化对消费者偏好的理解,进而实现精准的信息推送服务。该模式既帮助消费者快速筛选所需商品,又使企业能够提供针对性更强、效率更高、质量更优的服务[5]。

2.2. 精准广告投放行为的底层逻辑

作为一种完全以用户为中心的广告营销模式,这种一对一的广告投放在效率及精准度上大大超越了传统广告行业[6]。这种支撑服务器与客户终端浏览器实现的信息交互的是基于消费者的浏览历史记录和消费者个人终端中 Cookies、Brows History 等数据[7]。具体来说,当用户浏览某个网页时,服务器会在客户本地终端(包括电脑、智能手机等)的浏览器端相应地存储一个文本文件,如网络用户使用“抖音”搜索“减肥”之后,字节的搜索服务器就会读写并储存一条“减肥”的 Cookie,并保存在本地移动设备上。当用户再次访问搜索引擎时,浏览器会自动将存储的 Cookie 信息发送至服务器。网络服务提供商利用这些数据构建用户数字画像,并通过数据分析技术对访问者进行分类标记。例如,在抖音平台中,系统通过读取历史 Cookie 文件,可自动识别用户对“减肥”相关内容的偏好。由于 Cookie 能够持续记录并反馈用户的网络行为轨迹(包括浏览偏好和搜索历史),商家可借此精准定位目标人群,推送与其兴趣高度匹配的商品信息。具体而言,抖音的广告系统会扫描设备中的 Cookie 数据,提取“偏好设置”并传输至广告投放平台。通过智能匹配算法,平台会将带有“减肥”“瘦身”等标签的广告精准投放到短视频广告位中。本质上,网络服务商通过 Cookie 技术收集的用户实时行为数据,构成了行为追踪和定向广告投放的核心数据基础。

个人信息的汇集成为用户画像,我们成为了数据意义上的“透明人”,但这还不够骇人,现实情况往往是:一者,当你被贴上“肥胖”的标签,大数据会将“肥胖人群”的群体画像特征转嫁给你,也许你只是一时所好搜索“oversize”,但淘宝之后会铺天盖地地推送包含减肥药、瘦腿神器等与你毫不相干的广告。二者,当我们在百度搜索“减肥”之后,抖音、淘宝便会化身先知,开始推送“减肥”相关产品,关联共享下的精准广告,甚至不禁让我们怀疑李彦宏和马云的关系。致力寻求身份认知的大数据,反而成为人身与人格安全的威胁……

美国总统行政办公室提交的一份关于《规划数字化未来》的报告称:“从网络摄像头、博客、天文望远镜到超级计算机的仿真,来自于不同渠道的数据以不同的形式如潮水一般向我们涌来。如何收集、保存、维护、管理、分析、共享正在呈指数级增长的数据是我们必须面对的一个重要挑战。”²剖开精准广告为用户提供更多消费选项与便利的表象,定向投放的底层逻辑是大数据下个人信息的无所遁形与现实的丧失。谁动了你的 Cookie? 基于 Cookie 的精准广告行为是否合法? 我们不妨转向正当性的讨论。

¹Federal Trade Commission (2010). FTC regulation of behavioral advertising.

²转引,原文来自徐子沛:《大数据》,广西师范大学大学出版社2012年版,第87页。

3. 精准广告投放行为正当性分析

3.1. 隐私权与个人信息权的规范分析

作为广告发展的一种新模式，精准广告的投放以个人数据的收集与利用为基础，这就难免会与隐私权的保护产生冲突[8]。但随着 2021 年个人信息法的出台，对互联网大数据侵权的解释不再限于传统的隐私权，而加入个人信息权这一武器。在精准投放行为中，以 Cookie 为主的信息，属于隐私还是个人信息的范畴？

在现有研究中，多数学者(2019 年以前)以隐私权破题。但个人作为社会成员，隐私权的保护必然有所界限，不能因无限放大个人私生活的边界，而使社会中的其他人无所适从。代入“合理期待”原则，作为隐私权的客体，应当是该主体以及他所处的社会普通人群通常都会期待具有私密性、不愿意被公开的隐私[9]。但随着大数据的广泛使用，人们对合理期待的范围也随之改变。浏览器中的搜索是否属于合理期待？以朱烨诉百度侵权案为例，³“堕胎”是客观的“隐私”，私人电脑也理应属于“隐私场所”，但原告未采取相应措施如通过修改浏览器设置拒绝 Cookie 追踪，认定为隐私明显扩大合理期待的范畴。另一方面，被允许使用的个人基础信息，如身高、体重并非传统意义上的“隐私”，但也不应被广告随意使用，以个人隐私难以实现保护。

转至个人信息权视角，个人信息权具有特定的权利内容，包括个人有权了解谁在搜集其信息资料，搜集了怎样的信息资料，搜集这些信息资料从事何种用途，所搜集的信息资料是否客观全面，个人对信息资料是否有自我利用或允许他人利用的权利等[10]。与隐私权要求他人不作为，仅作为消极性的防御权利不同，个人信息权是允许何人使用、如何适用个人信息的主动权利。

对精准投放行为来说，商家往往需要以掌握用户大量信息为基础，最为常见的即追踪用户位置、通讯录、收集 Cookies、个人注册信息并进行使用。即完全属于《个人信息保护法》第四条对个人信息处理的范畴。

3.2. 个人信息权与隐私权的理论区分

3.2.1. 权利属性的区分

个人信息权与隐私权虽然在实践中存在交叉，但其法律属性存在明显区别。王利明教授指出，隐私权是一种“精神性的人格权”，主要体现的是个人的精神利益，侵害隐私权通常导致的是精神损害。而个人信息权则是一种“综合性权利”，既包括精神利益，也包括财产利益。这意味着个人信息权不仅保护个人的私密性，还保护其信息的商业价值，如姓名、肖像、健康信息等的使用和控制。因此，个人信息权具有更强的主动性，权利人不仅可以被动防御侵权行为，还可以主动授权他人使用其信息进行商业活动。

3.2.2. 权利客体的区分

隐私权的客体主要是“私密空间”“私密活动”和“私密信息”，强调的是个人不愿公开的私生活内容。而个人信息权的客体则是“身份识别性”信息，如姓名、身份证号、电话号码、健康信息等，这些信息可以单独或与其他信息结合识别特定自然人。因此，隐私权的保护范围相对狭窄，主要针对的是个人不愿公开的私密信息，而个人信息权则更广泛，涵盖所有具有识别性的信息。

3.2.3. 权利内容的区分

隐私权的核心在于“保密”，即防止他人非法获取、传播或利用个人的私密信息。而个人信息权的

³江苏省南京市中级人民法院(2014)宁民终字第 5028 号民事判决书。

核心在于“控制与利用”，即个人有权决定其信息的收集、使用、处理和披露方式。例如，个人信息权包括知情权、访问权、更正权、删除权等，这些权利在欧盟《通用数据保护条例》(GDPR)中得到了明确规定。相比之下，隐私权的保护方式更多是事后救济，如通过侵权责任法追究侵权责任。

3.2.4. 权利主体的区分

两者在权利主体上均限于自然人，不包括法人。这表明，隐私权与个人信息权的主体范围是一致的，但个人信息权的保护对象更广泛，不仅包括私密信息，还包括非私密信息。

3.3. 确立个人信息保护范围

相较于传统的大众媒体广告投放模式，基于用户画像的定向广告(Targeted Advertising)通过算法匹配实现了更高的信息相关性。这种精准营销模式在提升广告转化率的同时，也因其对用户行为数据的深度采集与分析，带来了更为显著的个人信息安全隐患[11]。当 Cookie 进入网络服务提供者的数据库，哪些属于个人信息？哪些可以用？哪些不能用？该怎么用？

个人信息分为敏感个人信息和详细个人信息。敏感个人信息，即涉及个人隐私的信息。根据英国 1998 年《资料保护条例》的规定，敏感个人信息是“由资料客体的种族或道德起源，政治观点，宗教信仰或与此类似的其他信仰，工会所属关系，生理或心理状况，性生活，代理或宣称的代理关系，或与此有关的诉讼等诸如此类的信息组成的个人资料。”与之相反的，详细个人信息则倾向于指代“很明显的没有导致被记录者的隐私权受到不当侵害的资料”。⁴

就网络服务提供者的收集与使用行为来说，针对一般琐细信息，如用户的身份证号(实名制)、姓名等，应通过公开披露的方式满足其知情权、控制权；而针对特殊敏感信息，如精准位置、通讯录、麦克风等则需要履行“明示同意”等较重的义务。

3.4. 匿名化与不可识别的联系

在朱烨诉百度侵权案中，二审法院即以“数据信息的匿名化特征不符合‘个人信息’的可识别性要求”为由进行了改判。笔者认为，匿名化不等于不可识别，匿名的信息处理依旧无法脱离个人信息的范畴。

大数据因其超强的信息收集、整合和挖掘、预测能力使数据的二次利用变得可行[12]。在大数据时代，算法技术的复杂性和不透明性导致了显著的信息不对称问题：网络服务提供者依托其技术优势，构建了一套用户难以理解和干预的数据采集体系。在这种权力结构下，用户往往处于三重认知盲区：数据采集范围的不确定性 - 无法知晓被收集的个人信息类别；数据流通过程的模糊性 - 难以追踪信息的传播范围与接收主体；数据应用方式的隐蔽性 - 不了解信息如何通过算法建模形成用户画像。

需要特别强调的是，这种“不知情”状态并不构成侵权行为的免责理由。根据个人信息保护法的基本原理，“告知 - 同意”原则要求数据控制者确保用户对其信息处理活动具有充分且真实的认知。算法黑箱导致的知情权缺失，本质上是对用户自主决定权的剥夺。

同理，由于脱敏与再识别技术的广泛应用，尽管网站在收集信息时进行匿名化处理，但用户在线行为所形成的 Cookie 集合依旧形成了一个“虚假”的用户画像，这个“用户”可以叫张三、可以是李四，但他的消费偏好、群体特征依旧可识别为电脑手机前的我们。从意识领域来说，尽管机器对这位“肥胖学生”是谁并不关注，但通过其处理信息推送的广告已经对我本人人格进行了伤害，这种“匿名化”依旧形成了个人信息的间接识别。

⁴转引，原文来自齐爱民：《拯救信息社会中的人格》，北京大学出版社 2009 年版。

3.5. 免责事由的阻却的意义

针对个人信息的侵权，主要体现在用户知情权与选择权及信息控制权两方面。

首先，网络服务提供者是否尽到足够或合理的告知义务？在 APP 注册界面时，用户与平台往往需要签订《隐私保护协议》。但实际来看，一方面多数网站的隐私声明未设置在具体显眼的位置，且一些专业术语晦涩难懂，更有甚至明确表示如果不同意该隐私政策，则无法安装使用该 APP，一般网络用户不太可能注意到层级如此之深的声明内容，尤其是有关用户个人隐私内容的格式化免责声明内容，网站应负有较高的提醒义务而非仅仅默示许可[13]。

其次，默示许可是否正当？Cookies 所带来的最大问题，是在用户完全不知情的状态下(除非预先在浏览器选项中手动将 cookies 设置为禁用模式)，如百度可以直接关闭“个性化广告推荐”选项，对用户进行跟踪和记录，并可能引发第三方的介入[14]。但平台在采集或使用个人信息时，有意识地不严格界定隐私信息、敏感信息、脱敏信息等边界，不针对这些分类的数据执行不同等级的保护或限制措施。如抖音需要打开位置功能以显示 IP，但同样也利用这一数据进行地区化广告推荐，或者将一些需要留痕的琐细个人信息与不想留痕的敏感个人信息“捆绑销售”，严重损害用户选择权；不仅如此，针对二次使用现象，即收集信息之后用作个性化广告推荐，尤其是与合作平台共享用户偏好设置则侵犯个人信息控制权。

3.6. 个人权利与社会需要的关系

网络社会中引发的种种问题，归根结底是网络空间中个人权利与社会需要之间的冲突[15]。精准广告投放确实为用户提供了筛选海量信息的便利，并使其能够免费使用相关服务。然而，平台通过收集用户的 Cookie 数据进行广告投放，并与第三方网站合作推广，其主要动机仍是商业利益最大化，而非公共利益。此外，这种默示授权的 Cookie 使用机制可能不仅涉及财产性权利，还可能触及个人隐私权，存在一定的法律和伦理风险。

用户对精准广告的接受度并非无限，其容忍阈值取决于隐私成本与信息收益的平衡。当用户感知到的隐私侵害风险超过其从精准投放中获得的便利时，便可能触发对平台侵权行为的质疑与抵制[16]。精准定向广告推送不断透视个人隐私的过程，好比用个人人格换取一时便利的过程。个人信息的保护可以为科技发展与社会需要让步，但人格的保护也不容忽视。正如朱松林教授所说：“立法机构在制定网络行为定向广告管理措施时，应该综合考虑技术带来的积极和消极影响，起草出一部宽严适度的负责任的规制法案，既能促进网络经济的创新发展，又能最大程度地保护消费者的利益。”[17]

3.7. 精准广告投放行为的法律性质与正当性分析

3.7.1. 精准广告投放的法律性质

精准广告投放是指通过收集用户的行为数据、浏览记录、地理位置等信息，进行个性化推荐和定向广告投放的行为。这种行为在法律上属于“自动化决策”或“行为定向广告”，其法律性质主要涉及个人信息的收集、使用和披露是否合法。

根据《中华人民共和国民法典》第 111 条，个人信息受法律保护，任何组织或个人不得非法收集、使用、加工、传输个人信息，不得非法提供、公开个人信息。同时，《个人信息保护法》第 24 条明确规定，通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。这表明，精准广告投放虽然具有商业价值，但必须在合法、正当、必要的前提下进行。

3.7.2. 精准广告投放的正当性

精准广告投放的正当性主要体现在以下几个方面：

合法性：广告投放必须基于合法目的，如提供相关服务、履行合同义务等。如果广告投放超出合理范围，如未经用户同意收集非必要信息，则可能构成违法。

正当性：广告投放必须符合“正当性”原则，即信息的收集和使用必须与用户的真实需求相关，不能以“精准”为名进行过度收集或滥用。

必要性：广告投放必须基于“最小必要”原则，即只收集和使用必要的信息，不得过度收集或滥用。

用户知情与同意：用户有权知晓其信息被收集、使用的方式，并有权拒绝或撤回同意。《个人信息保护法》第 24 条要求提供便捷的拒绝方式，以保障用户的知情权和选择权。

4. 精准广告治理的法律路径

4.1. 细化立法：“告知 - 同意”模式的完善

针对网络服务提供者对用户个人信息的收集，从 2014 年的《中国互联网定向广告用户信息保护行业框架标准》到 2021 年的《个人信息保护法》甚至于司法实践，通行的都是“告知 - 同意”模式。但模式适用情形模糊，个案依旧个案分析，起不到实际作用，亟待完善。

当前普遍采用的“告知 - 同意”机制存在明显的操作壁垒：用户必须通过主动干预——在平台设置中手动禁用 Cookies 或个性化广告推荐功能，方可避免在线行为被追踪。这种“默认允许 + 主动退出”(opt-out)的设计模式，实质上将隐私保护的责任完全转嫁给用户，而非由平台承担默认的隐私尊重义务[18]。但在实际应用中：一者，平台最初公开的《隐私保护政策》往往夹杂在众多协议之中，条文冗长、晦涩难懂。二者，禁用 Cookies 或隐私权限等选项默认都是开启状态，且藏匿颇深，关闭之后可能导致一些功能无法正常使用。三者，部分隐私协议被设置成格式条款、“捆绑销售”，不同意则无法使用 APP。

看似尊重用户知情权与选择权的模式与协议，却被运营商花样百出的裹挟手段打败。从立法来说，应对涉及“告知 - 同意”的条款进行位置明显、条文简单明确地公示，并禁止出现相关格式条款，对于用户主动关闭 Cookie 等个性化推荐功能的，不能籍此进行其他功能的限制。

4.2. “告知 - 同意”模式的适用性分析

“告知 - 同意”模式是个人信息处理中的核心法律机制，其适用范围广泛，涵盖从收集、存储、使用到共享、转让等各类个人信息处理活动。根据《信息安全技术个人信息处理中告知和同意的实施指南》(Protiviti)的分析，该模式在不同场景下具有不同的适用要求，例如在 APP 基本业务功能与拓展业务功能、第三方 SDK 嵌入、未成年人信息处理、个性化推送、云计算服务等场景中，均需明确告知内容并获得用户同意。这表明，“告知 - 同意”模式并非适用于所有情况，而是需要根据具体业务场景进行灵活适用。

同时，“能够够用和必要原则”作为《个人信息保护法》的核心原则之一，强调在收集个人信息时应限于实现处理目的的最小范围，不得过度收集。例如，学校在收集学生个人信息时，应坚持“最小、够用、必要”的原则，拒绝不合理的要求，并通过学校的力量积极呼吁社会各界保护学生信息隐私。这一原则的适用性不仅体现在数据收集环节，也应贯穿于数据处理、存储、使用等全过程。

4.3. “告知 - 同意”模式的细化建议

4.3.1. 明确告知场景与内容

在“告知 - 同意”模式中，告知的场景和内容应根据具体业务场景进行细化。例如，在 APP 中，应区分基本功能与拓展功能，对基本功能的个人信息处理应进行基础告知，而拓展功能则需提供更详细的告知内容。此外，对于涉及未成年人、敏感信息处理等特殊场景，应采用更明确、更易理解的方式进行告知，如通过弹窗、语音提示等方式，确保用户能够充分理解其权利与义务。

4.3.2. 规范同意机制

“同意”机制应具备可操作性，避免“同意”流于形式。例如，用户应能够通过简单、便捷的方式撤销同意，且系统应记录用户同意的撤回情况。此外，对于涉及未成年人的个人信息处理，应采用“双人同意”或“监护人同意”机制，以确保未成年人的隐私权不受侵害。同时，应鼓励用户通过“一键同意”或“默认拒绝”等方式，提升用户体验与操作便捷性。

4.3.3. 细化“能够够用和必要原则”的适用

在实际操作中，应建立“能够够用和必要原则”的评估机制，确保个人信息收集的最小化。例如，在教育领域，学校在收集学生信息时，应根据实际教学需求，评估是否需要收集额外信息，如是否需要收集学生家庭住址、联系方式等非必要信息。此外，应建立信息收集的审批流程，确保信息收集的必要性合理性，并通过定期评估机制，确保信息收集的持续合规性。

4.3.4. 加强个人信息保护的配套措施

在“告知-同意”模式和“能够够用和必要原则”之外，还应配套其他个人信息保护措施，如数据加密、访问控制、数据匿名化等，以形成完整的个人信息保护体系。例如，在医疗领域，应通过数据加密和访问控制，确保患者信息的安全性；在金融领域，应通过数据匿名化和最小化处理，确保用户信息的隐私性。

4.4. 行业规制：能够够用和必要原则的适用

至于能够够用和必要原则的适用，则主要针对用户的信息控制权。现实情况是：网络服务提供者会将确实需要的琐细个人信息与非必要的敏感信息混杂，一同申请用户同意。如微信登录公众号除要求用户的头像、账号等，还需要通讯录权限。无独有偶，也会以 A 理由收集个人信息后，将其使用在 B 功能之上，如抖音要求用户公开位置信息获取 IP 地址，但位置信息也用于同城广告的投放。不仅如此，用户共享协议，即使用 A 公司偏好设置后，与 A 公司共享数据的 B 公司也出现相似推荐。

从立法来说，细化不同类型的个人信息，针对类型进行不同程度的保护，如对通讯录等敏感信息赋予最高标准的同意权限；另外，对于“搭便车”的个人信息收集侵权，针对不同类型功能的运营商出台相关细则，并明文规定在《隐私保护协议》中，并进一步认定相关侵权责任。

5. 结论

霍金曾说，我们正在进入一个以大数据为起点而非终点的时代。正如大数据技术一样，精准广告地投放并非自出生伊始便带有“原罪”。恰恰相反，在倡导用户免费使用、增加广告收益的互联网经营中，精准广告为消费者与广告主双方都带来了便利。但当我们沉醉于挖掘个人信息这一“富矿”时，获取消费者信任，保障用户人格权利依旧是互联网广告治理的“重头戏”。实现保护个人权利与满足社会需要间的利益平衡，完善个人信息保护法，更是数字法治孜孜以求的目标。

参考文献

- [1] 迈尔·舍恩伯格, 库克耶. 大数据时代[M]. 盛阳燕, 周涛, 译. 杭州: 浙江人民出版社, 2013.
- [2] 陈纯柱, 王唐艳. 大数据时代精准广告投放的隐私权保护研究[J]. 学术探索, 2020(4): 105-112.
- [3] 范炜, 李仁杰, 王颖. 基于大数据的精准广告投放[J]. 中国有线电视, 2018(1): 12-14.
- [4] 朱巍. 网络精准营销与隐私权保护分析[J]. 人民法院报, 2014(3): 17-22.
- [5] 戴世富, 赵思宇. 隐性与隐私: 原生广告的伦理反思[J]. 当代传播, 2016(4): 98-100.
- [6] 卜时忠. 网络精准营销下的网络隐私权的保护[J]. 市场周刊(理论研究), 2013(4): 36-37.

-
- [7] 刁生富, 赵亚萍. 网络环境下精准定向广告推送与隐私权保护[J]. 淮阴师范学院学报(哲学社会科学版), 2018, 40(5): 524-527+540.
- [8] 张晓阳. 基于 Cookie 的精准广告投放技术及其法律边界刍议以朱烨诉百度公司隐私权纠纷为视角[J]. 电子知识产权, 2015(9): 81-87.
- [9] 杨秀. 大数据时代定向广告中的个人信息保护——《中国互联网定向广告用户信息保护行业框架标准》分析[J]. 国际新闻界, 2015, 37(5): 138-155.
- [10] 王利明. 论个人信息权的法律保护[J]. 现代法学, 2013(4): 64-65.
- [11] <http://www.jmstandard.org.cn/Article/ShowArticle.asp?ArticleID=2587>
- [12] 徐明. 大数据时代的隐私危机及其侵权法应对[J]. 中国法学, 2017(1): 130-149.
- [13] 王菲. 互联网精准营销的隐私权保护: 法律、市场、技术[J]. 国际新闻界, 2011, 33(12): 90-95.
- [14] 石佳友. 网络环境下的个人信息保护立法[J]. 苏州大学学报(哲学社会科学版), 2012, 33(6): 85-96.
- [15] 徐瑞萍, 刁生富. 论网络空间中的隐私权[J]. 自然辩证法研究, 2004, 20(11): 79-82.
- [16] 沈维梅. 网络精准广告的发展及困惑[J]. 新闻界, 2010(1): 184-185+144.
- [17] 朱松林. 论行为定向广告中的网络隐私保护[J]. 国际新闻界, 2013, 35(4): 94-102.
- [18] 朱芸阳. 定向广告中个人信息的法律保护研究——兼评“Cookie 隐私第一案”两审判决[J]. 社会科学, 2016(1): 103-110.