理论前沿

用户画像、个性化推荐与个人信息保护

丁晓东

内容提要:网络社会中的用户画像与个性化推荐已经越来越普遍,对个人信息保护提出了挑战。通过分析,可以发现网站对用户匿名行为信息收集常常存在不规范的情况。一方面,应当将用户匿名行为信息纳入个人信息的范畴,确保用户画像与个性化推荐中用户的知情权与拒绝权;另一方面,应当将用户匿名行为信息和已识别个人信息区别对待,采取特殊的个人信息保护机制。规制用户画像与个性化推荐中的信息收集与使用,应当要求企业承担更多的治理责任,保障用户的信息质量与信息安全。在用户匿名行为信息收集阶段,应当允许企业在用户明确同意或可预期的前提下进行信息收集;在信息的汇聚融合与用户画像阶段,应当要求企业承担相应的数据信息安全保障义务;在信息利用与个性化推荐阶段,应当要求企业注意相关伦理规范,避免利用用户敏感信息进行推送。企业对用户匿名行为信息的收集、汇聚与利用应当采取基于标准而非规则的风险规制路径,避免套用一般性的个人信息保护法律框架。

关键词:用户画像　个性化推荐　个人信息保护　匿名化　风险规制

丁晓东,中国人民大学法学院副教授。

随着网络技术与信息技术的高速发展,用户画像与个性化推荐已经越来越普遍。在商业领域,越来越多的企业开始收集个人的浏览记录、购买记录、交易方式等信息,依据这些信息来分析用户行为,对网络用户进行用户画像和精准营销。用户画像与个性化推荐促进了互联网经济的发展,在很多情形下,它们使得商家可以更为精准地投放广告;同时,它们也使得消费者可以获取更为有效的商品信息。

用户画像与个性化推荐也对用户相关权益的保护提出了挑战。很多专家指出,个人消费行为信息属于个人信息的范畴,在未经个体明确同意与授权的情形下,对于此类个人信息的收集与利用侵犯了用户的相关隐私权益。在国外,对于用户画像与个性化推荐也存在争议。在美国,对于网络用户的消费行为信息是否属于个人信息,一直存在不同的观点。在有的企业看来,用户的消费习惯信息不属于个人信息,因为不能根据此类信息识别

特定的个体。而且,企业在收集了此类信息后,一般会将此类信息进行匿名化处理。但在其他人看来,此类信息属于个人信息,因为此类信息本身就是对个人的识别,而且结合其他信息,此类信息甚至可以经常定位到具体的个体。欧洲对于个人信息的界定范围较为宽泛,而且相关法律直接将用户画像纳入了规制范围,例如2018年生效的《一般数据保护条例》(本文简称《条例》)第4条第(4)款规定,"为了评估自然人的某些条件而对个人数据进行的任何自动化处理,特别是为了评估自然人的工作表现、经济状况、健康、个人偏好、兴趣、可靠性、行为方式、位置或行踪而进行的处理"都属于用户画像,都受《条例》的管辖。但如何解释《条例》中的相关条款,以及如何从原理层面分析这些条款,仍然有待进一步讨论。

一 网站如何收集与利用信息:技术问题与法律挑战

在企业对个人信息的收集中,通过网站来收集个人信息是极为重要的一种途径。了解网站收集个人信息的途径,这将为思考用户画像、个性化推荐与个人信息保护问题打好基础,保证相关理论探讨更具有现实关切。

(一)网站收集个人信息的技术

就网站获取用户信息的方式来说,其首选是要求用户进行注册,通过用户的注册、登录来创建用户数据库,标记所有的用户。通过此种方式,网站可以很好地对用户的个人信息进行管理,例如网站常常会生成一个含有唯一标示符的信息,并通过这个信息将用户的所有行为关联起来。例如用户浏览的网站、点击的行为、购买的商品,网站可以对这些信息进行收集与追踪,并对个体进行用户画像与精准营销。

但一般来说,以用户名的方式来收集用户的信息比较适用于需要登录才能实现完整服务的网站或软件(例如微信、淘宝、QQ)。对于很多没有形成完整闭环的网站或软件(例如搜索引擎类网站和新闻类网站),用户常常不会主动注册和登录,也因此网站就很难使用用户登录的方式对个体进行信息的收集与追踪。此外,即使一些形成闭环的网站,用户也可能仅仅行使浏览功能,此时网站也无法经由用户登录而收集信息。

但网络用户常常会有这样的体验,即使没有注册或登录某个网站,网站也常常可以实现个性化推荐或营销。当我们在某个电商网站上搜索和浏览了某些产品后,在"你可能感兴趣"的一栏中就会出现和我们之前搜索与浏览记录相关的产品。此类个性化推荐和营销之所以可能,是因为网站具备了很多技术手段,可以实现对非注册用户的追踪与管理。综合而言,比较常用的技术包括了如下几种:

1. **HTTP Cookie**

网站跟踪和收集用户信息的最常用方式是HTTP Cookie或Cookie技术。Cookie技术之所以被广泛应用,最主要的原因是因为Cookie技术可以帮助服务器知道用户上一次的操作是什么,从而帮助交互式Web应用程序的功能实现。例如当用户在某个页面上将购买的商品放入了购物车,然后点击结算页面跳入到下一个网页,此时如果没有Cookie技术,服务器就不知道用户放入购物车的物品是什么。但在Cookie技术的帮助下,这种难

题就解决了。在用户开启 Cookie 的情况下，网站可以在用户计算机上设置一个跟踪的 Cookie，以某个特定的标记来识别某台计算机（例如 1234abcd），这样，当用户进入到结算页面，网站也可以知道用户此前放入购物车的商品是什么。[1]

由于 Cookie 技术可以在用户计算机上设置文件，维持用户与网站的对话，网站也因此获得了收集与追踪用户行为信息的机会。只要用户开启 Cookie，并且没有删除浏览器中保持的 Cookie ID，网站就可以持续性地访问 Cookie 并获取保存在 Cookie 中的信息。当然，一旦用户关闭 Cookie，网站就无法通过 Cookie 技术来为用户提供服务/收集 Cookie 信息；当用户删除浏览器中的 Cookie ID 时，网站也无法访问之前 Cookie 中所保持的信息。

对于 Cookie 的利用常常并不来自于同一个网站。[2] 用户往往会误以为网站都是单一构成的，某个网站都是由同一家网络公司所提供的。但事实上，网站常常由不同的网络公司提供。例如一家新闻类的网站，其天气预报的内容可能是由某天气预报网站提供的，其广告可能是由某网络广告商提供的。在收集与追踪用户的信息时，不仅仅是用户访问的网站，而且包括天气预报网站与网络广告商都可能访问用户电脑中的 Cookie 文件，收集 Cookie 中的信息，并对用户进行画像。[3]

2. **Flash Cookie**

Cookie 技术可以实现网站对登录 ID、使用偏好、习惯的收集，但一旦用户行使网页浏览器中的“删除历史记录”时，网站就无法持续地追踪用户。此外，对于用户没有访问过的网站，此类网站也不可能通过 Cookie 技术收集用户信息。要在以上情形中仍然实现对用户信息的收集与追踪，需要借用 Flash Cookie 技术。

所谓“Flash Cookie”，技术上又可以称为“本地共享对象（local shared objects）”，是由 Adobe Flash 开发人员使用用户的计算机上存储数据的文件。[4] 相比起普通 Cookie 技术，Flash Cookie 技术的存储空间更大，[5] 储存时间更长，[6] 储存位置对于普通人而言更难发现。[7] Flash Cookie 的这些技术特征使得其在追踪与收集用户信息方面更具有优势。在使用 Flash Cookie 的情形下，即使用户删除了其历史浏览记录，或者即使用户改用了不同的浏览器来访问网站，被访问的网站将仍然可以追踪和收集个人信息。

---

〔1〕 具体实现方式 Cookie 是由服务器端生成（webserver 或者 cgi），反馈给用户的浏览器，用户浏览器会将 Cookie 的 key/value 保存到某个目录下的文本文件内，下次请求同一网站时就发送该 Cookie 给服务器（前提是浏览器设置为启用 Cookie）。

〔2〕 See Güneş Acar (et. al.), Facebook Tracking Through Social Plug-ins, https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf, 最近访问时间 [2018-09-25]。

〔3〕 See Interactive Advertising Bureau, A Guide to Online Behavioral Advertising, www.iabuk.net/sites/default/files/publication-download/OnlineBehaviouralAdvertisingHandbook_5455.pdf, 最近访问时间 [2018-09-25]。

〔4〕 See Ashkan Soltani (et. al.), Flash Cookies and Privacy, http://ssrn.com/abstract=1446862, 最近访问时间 [2018-09-28]。

〔5〕 Cookie 仅允许存储 4KB，而 Flash Cookie 则允许存储 100KB。此外，Flash Cookie 还可以自行调整存储空间大小。

〔6〕 Cookie 有消亡期，它会在一段时间后自动消失；而 Flash Cookie 如果没有主动删除，则会永久保持在用户电脑上。

〔7〕 用户并不需要 Cookie 的位置即可删除 Cookie，可以有很多方式和软件对其进行一次性删除，所有浏览器本身都内置了这一功能。而 Flash Cookie 则是存储在 C:\Documents and Settings\用户名\Application Data\Macromedia\Flash Player 文件夹下。其中#sharedobjects 文件夹用于存储 Flash Cookie，macromedia.com 存储 Flash Cookie 的全局设置。对此一般用户很难知晓。

3. **Ever Cookie**

Ever Cookie 技术可以更多地对 Cookie 进行储存，而且相比起普通 Cookie 与 Flash Cookie，这种技术将使得网络用户更难删除其 Cookie，可以使网站能够更准确地辨识用户，对用户进行更为持续、稳定与准确的画像。

Ever Cookie 的技术手段主要在于尽可能地在用户电脑里进行备份，利用不同的储存机制来不断自我复制 Cookie，以及在副本丢失或到期后确保 Cookie 可以重新复活。[8] 这样，即使用户删除了其历史浏览记录，甚至删除了储存在电脑某个文件夹中的 Cookie 文件，网站也仍然可以在其他文件里发现 Cookie 的备份。通过 Ever Cookie 技术，可以让网站所标示的个人 Cookie ID 具有更高的稳定性和可识别性，排除算法本身随机性的影响。

基于 Ever Cookie 的此种特征，Ever Cookie 也被有的专家称为“僵尸 Cookie（Zombie Cookie）”。[9] 因为一旦使用 Ever Cookie 技术来追踪和收集用户的信息，用户就很难通过对 Cookie 的删除来防止自己的信息被收集。

4. **Fingerprinting**

Fingerprinting 技术通过交叉比对关键信息验证来识别计算机。就像在现实社会中人们可以通过指纹来识别特殊的个体一样，服务器在传输过程中可以利用传输的关键信息来识别某台计算机。[10] 例如某个网站可以识别用户使用的浏览器类型，用户使用的字体，以及网站在计算机上安装的插件。这些信息可能都不是唯一的，但是结合起来，它们可以识别唯一的个体。[11]

与前面几种 Cookie 技术不同的是，Fingerprinting 技术不直接在用户的电脑上储存文件。也因此，用户往往更难发现基于 Fingerprinting 技术的信息收集与追踪，也更能采取措施来避免此类信息收集与追踪。为了避免 Fingerprinting 技术对相关信息的收集与追踪，人们必须禁用网站的关键功能，例如 JavaScript 和 Adobe 的 Flash。

（二）法律争议

网站对于个人信息的各种收集与追踪技术合法吗，需要受到法律的规制吗？一般认为普通 Cookie 技术是合法的，是实现用户与网站对话的必要技术，但诸如 Flash Cookie、Ever Cookie 与 Fingerprinting 这类收集用户匿名信息的技术呢？是否应当对其进行禁用？或者在允许其使用的情形下，是否应当对其进行一定程度的法律规制？除了收集阶段，此类信息的汇聚也存在法律争议。当网站通过各种技术手段收集到此类信息后，它们就会在数据管理平台对此类信息进行同源化处理和分析，通过海量的数据实现信息的融合，最

---

〔8〕 具体来说，Ever Cookie 在创建 Cookie 时会使用如下存储机制：标准 HTTP Cookie；Local Shared Objects（Flash Cookie）；Silverlight Isolated Storage；以自动生成、强制缓存的 PNG 像素图片的 RGB 值形式保存 Cookie，使用 HTML5 Canvas 标签读取像素图片（Cookie）；在浏览器历史记录中存储 Cookie；在 HTTP ETag 中存储 Cookie；在浏览器缓存中存储 Cookie；window. name 缓存；Internet Explorer user Data；HTML5 Session Storage；HTML5 Local Storage；HTML5 Global Storage；HTML5 Database Storage（SQLite）。

〔9〕 See Christian Olsen，Supercookies：What You Need to Know About the Web’s Latest Tracking Devic（Mashable），http://mashable.com/2011/09/02/supercookies-internet-privacy，最近访问时间［2018-09-28］。

〔10〕 See Gunes Acar（et. al.），FPDetective：Dusting the Web for Fingerprinters，2013 *ACM Conference on Computer and Communications Security*，November 2013.

〔11〕 See Peter Eckersley，“How Unique Is Your Web Browser?”，6205 *Lecture Notes Ccomputer SCI*. 1（2010）.

终形成关联到具体用户或识别码的用户画像。对于此类数据融合,法律是否应当完全允许,还是应当对其施加一定的规制?最后,信息利用阶段也存在法律争议。若网站利用消费者匿名信息和用户画像进行个性化推荐,此类个性化推荐是否应当受到法律的某种规制?

要回答和解释这些问题,需要对其中最为核心的问题进行思考:用户的匿名行为信息是否属于个人信息?法律对于用户画像与个性化推荐应当采取何种立场?法律如何从个人信息保护的角度对待此类问题,将在很大程度上决定上述问题的答案。同样,如果法律对于用户画像与个性化推荐已经明确立场,那么上述法律争议也会有更为明确的答案。

二 比较法视野下的问题分析

从比较法的视野出发,可以发现针对网站利用消费者行为信息进行用户画像与个性化推荐,全球不同国家和地区采取了不同的规制方式。对于匿名化的消费者行为信息是否属于个人信息,不同规制机构、专家与学者也给出了不同的观点。

(一) 中国

我国目前对于网络用户画像和个性化推荐并没有直接的法律规定。对于网站使用 Cookie 等技术收集用户的行为信息,并且利用此类信息为个体进行个性化推荐,我国的法律并没有明确禁止。《电子商务法》第 18 条规定:"电子商务经营者根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务的搜索结果的,应当同时向该消费者提供不针对其个人特征的选项,尊重和平等保护消费者合法权益。"但这一规定并未直接规定网站收集与处理个人消费行为信息是否合法,而且对于这一规定的解读争议很大。

事实上,网站收集与利用消费者的行为信息大体上受到了法院的支持。2013 年,在朱烨诉百度公司隐私权纠纷案中,朱烨认为其在百度公司搜索"减肥""丰胸"等关键词后,会在浏览相应的网页时出现诸如"减肥""丰胸""人工流产"等广告,因此百度公司对于其消费行为信息的收集和利用侵犯了其隐私权。一审法院支持了朱烨的主张,[12] 但二审法院认为,百度公司收集的是不能识别用户个人身份的信息,此类数据不符合个人信息的可识别性要求;而且,相关网页只是对特定的用户进行推送,并没有公开用户的消费行为及其偏好,因此并没有打扰用户的安宁或对用户产生实质性损害。[13]

从个人信息的界定来看,我国的现行法律也并未完全明确消费者的行为数据是否属于个人信息。《网络安全法》第 76 条规定:"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。"从这一条的规定来看,似乎可以将用户的消费行为信息界定为个人信息,因为结合其他信息,此类信息很可能可以识别个体。但该法第 42 条又规定:"网络运营者不得泄露、篡改、毁损其收集的个人信息;未经被收集者同意,不得向他人提供个人信息。但是,经过处理无法识别特定

〔12〕 江苏省南京市鼓楼区人民法院(2013)鼓民初字第 3031 号民事判决书。

〔13〕 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。

个人且不能复原的除外。”对于匿名化的消费者行为信息，这条规定又似乎希望将用户的消费行为信息与其他可直接识别的个人信息进行区别对待。

一些技术标准似乎采取了较为宽泛的定义，将消费者的行为信息也纳入到个人信息的范畴。例如《信息安全技术个人信息安全规范》规定，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，如姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等”。根据这一定义，除了能够通过具体信息“识别”个人，“关联”也可以成为个人信息的范畴。“由特定自然人在其活动中产生的信息（如个人位置信息、个人通话记录、个人浏览记录）”也应当被视为个人信息。〔14〕

（二）美国

美国没有个人信息保护的统一立法，也没有联邦层面对网站利用消费者行为进行用户画像与个性化推荐的法律规制。但自从20世纪90年代以来，监管机构美国联邦贸易委员会（FTC）开始逐渐关注信息隐私的问题。1998年，联邦贸易委员会发布了一份报告，对商业网站披露用户隐私的做法进行了全面审查，并制定了“公平信息实践原则”。〔15〕根据这一原则，在收集个人信息时，“网站需要向消费者提供关于其信息实践的清晰和明显的通知，包括他们收集什么信息、他们如何收集信息（例如，直接或通过非显而易见的方式，例如Cookie）、他们如何使用它、他们如何向消费者提供选择、可访问性与安全，他们是否向其他实体披露收集的信息，以及其他实体是否正在通过网站收集信息。”〔16〕

在公平信息实践原则的指引下，联邦贸易委员会采取了基于透明性的监管原则，即在网站违反隐私政策收集个人信息，或者网站对个人信息收集不透明的情形下，联邦贸易委员会可以要求网站遵守信息收集透明的要求。例如2009年，联邦贸易委员会调查了零售商Sears公司。联邦贸易委员会认为，尽管零售商Sears公司已经向用户提供了一个隐私政策协议，但Sears公司没有充分披露其对付费客户的跟踪程度，没有告知其网站程序可能会跟踪和记录客户的浏览记录和习惯，因此已经构成了对消费者的欺骗。〔17〕联邦贸易委员会要求，Sears公司在其隐私政策协议中清晰地描述网站软件“将监视、记录或传输的数据类型”。〔18〕2010年，联邦贸易委员会又对EchoMetrix公司进行了调查。在EchoMetrix公司所设计的一款“家长控制”软件中，EchoMetrix公司对儿童电脑活动的数据进行了秘密跟踪，并将此类数据传输给了营销人员。〔19〕联邦贸易委员会认为，此类对于儿童信

〔14〕 GB/T 35273－2017《信息安全技术个人信息安全规范》，附录A。

〔15〕 公平信息实践原则早在20世纪六、七十年代就已经提出，而且奠定了现代信息隐私法的基本框架。参见丁晓东《论个人信息法律保护的思想渊源与基本原理》，《现代法学》2019年第3期，第96－110页。

〔16〕 See FTC, Privacy Online: A Report to Congress 7 (1998), http://www.ftc.gov/sites/default/files/documents/public_events/exploring－privacy－roundtable－series/priv－23a_0.pdf，最近访问时间［2018－10－08］。

〔17〕 See Sears Holdings Mgmt. Corp., F. T. C. Docket No. C－4264 (Aug. 31, 2009).

〔18〕 Decision and Order at IA, Sears Holdings Mgmt. Corp., F. T. C. Docket No. C－4264 (Aug. 31, 2009).

〔19〕 See FTC v. EchoMetrix, Inc., No. CV10－5516 (E. D. N. Y. Nov. 30, 2010).

息的追踪与披露是不透明的，没有获取消费者的同意。[20]

在 2010 年 12 月的一份报告中，联邦贸易委员会又提出了新的消费者数据隐私监管框架，主张设立一个统一和全面的“不跟踪(DO NOT TRACK) ”机制。[21] 根据该机制，当网站追踪和收集消费者的行为信息时，应当为消费者提供“统一和全面的消费者选择机制”，赋予消费者拒绝用户画像与个性化推荐的权利。具体来说，应当在“消费者的浏览器上放置持久性的 Cookie 设置，并将该设置传送至消费者所访问的网站，以明确地确定消费者是否希望被跟踪或收到个性化的广告”。[22] 联邦贸易委员会认为，“不跟踪”机制将优于现有的基于浏览器的 Cookie 设置，因为它“更清晰、更容易找到和更有效”，而且它直接将选择退出的机制设置在被访问的网站上。[23]

但是，联邦贸易委员会的监管建议并未上升为立法。联邦贸易委员会曾经在 2011 年左右在国会听证，建议采取更严格的措施以规制未经授权的用户画像与个性化推荐，包括采取“不跟踪”机制。[24] 但国会并未采纳贸易委员会的主张。此外，国会曾经提出过的一些法案虽然都主张对用户画像和个性化推荐进行监管，但最终也都未能成为法律。

(三) 欧盟

欧盟对于网络用户画像与个性化的规制要明确很多。自 2009 年起，《电子隐私指令》就对 Cookie 的使用做出了详细的规定: 凡是在用户的电脑上储存信息，或者访问用户电脑上的信息，不论此类数据是否属于个人数据，都必须获得用户的同意。[25] 例外的情形只有为了传输数据或者用户提出服务所必要。专门负责对欧洲数据隐私提出建议的第 29 号工作小组指出，用户的同意必须是明确同意，[26] 不能是默认同意。[27] 2017 年，欧盟又提出以《电子隐私条例》替代《电子隐私指令》，[28] 但对于使用 Cookie 等技术获取信息，《电子隐私条例》延续了之前的规制立场，只是在某些方面做出了调整。[29]

此外，《条例》也规定了用户画像与个性化推荐的限制。《条例》第 21 条第 1 款规定，

---

[20] See FTC v. EchoMetrix, Inc. , No. CV10 - 5516 (E. D. N. Y. Nov. 30, 2010) , pp. 16 - 18.

[21] See FTC, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (December 1, 2010) , http: //www. ftc. gov/os/2010/12/101201privacyreport. pdf，最近访问时间 [2018 - 10 - 08]。

[22] FTC, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, p. 66.

[23] FTC, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, p. 67.

[24] See Shelton and Clinton J. McCord, How to Respond to Recent Developments in Consumer Information Regulation, http: //www. wildman. com/bulletin/3232011/，最近访问时间 [2018 - 11 - 08]。

[25] Privacy and Electronic Communications Directive 2009/136/EC, article 5 (3) .

[26] See Article 29 Working Party, Opinion 15/2011 on the Definition of Consent (WP 187) , pp. 32, 35, https: //www. pdpjournals. com/docs/88081. pdf，最近访问时间 [2018 - 11 - 11]。

[27] 对此也存在争议。See Eleni Kosta, Peeking into the Cookie Jar: The European Approach towards the Regulation of Cookies, 21 *International Journal of Law and Information Technology* 4, 17 (2013) .

[28] See Regulation on Privacy and Electronic Communications, https: //ec. europa. eu/digital - single - market/en/news/proposal - regulation - privacy - and - electronic - communications，最近访问时间 [2018 - 12 - 08]。

[29] 《电子隐私条例》对于 Cookies 的规定要更简洁，而且要求 Cookies 获取用户同意的方式应当更便捷。See Regulation on Privacy and Electronic Communications, article 10.

当处理数据主体的数据时，“包括根据这些条款进行的用户画像，数据主体应当有权随时反对”。[30] 第21条第2款和第3款进一步规定“当因为直接营销目的而处理个人数据，数据主体有权随时反对为了此类营销而处理相关个人数据，包括反对和此类直接营销相关的用户画像”；“当数据主体反对为了直接营销目的而处理，将不能为了此类目的而处理个人数据”。[31] 根据《条例》第21条的规定，也可以比较明确地确定网站收集与处理个人的行为信息属于法律调整的范围，网站的此类活动必须明确获得用户的同意，而且应当保证用户有权随时反对和拒绝网站对其进行画像与个性化推荐。

欧盟1995年制定的《数据保护指令》（本文简称《指令》）指出，个人数据指的是“任何已识别或可识别的自然人（‘数据主体’）相关的信息，一个可识别的自然人是一个能够被直接或间接识别的个体，特别是通过诸如身份编号或个体的身体性、生理性、精神性、经济性、文化性或社会性身份而可以直接识别或间接识别”。[32] 欧盟法院曾经依据《指令》明确做出解释，指出没有姓名的信息也可以构成个人数据。[33] 而第29号工作小组在其对个人数据的解释中，也将可能识别个人的消费行为数据也纳入了个人数据的范畴。[34]

《条例》替代了《指令》。但就个人数据的范围而言，其范围反而比之前的《指令》更广了。《条例》除了延续《指令》的定义，还把“姓名、身份编号、地址数据、网上标识”等数据明确列为个人数据的范畴。[35] 而且，《条例》条文的详述明确指出，只要采取“所有可能合理使用的手段来直接或间接挑出”个体，此类个体就属于可识别的个体。即使某些数据被匿名化处理，但“只要通过额外的信息可以追踪到个体，此类数据就可以被视为一个可识别自然人的信息”。[36] 由此可见，在欧洲，基本的共识是匿名化的用户消费者数据应当属于个人信息。[37]

三　支持理由与反对理由

对于法律是否应当规制用户画像与个性化推荐，是否应当将用户的匿名行为信息纳

---

〔30〕 例外情形是“除非控制者证明，相比数据主体的利益、权利和自由，具有压倒性的正当理由需要进行处理，或者处理是为了提起、行使或辩护法律性主张。”参见《条例》第21条第1款。

〔31〕 《条例》第4款进一步规定了用户的知情权“至晚在和数据主体所进行的第一次沟通中，第1款和第2款所规定的权利应当让数据主体明确知晓，且应当与其他信息区分开来，清晰地告知数据主体。”参见《条例》第21条第4款。

〔32〕 The Data Protection Directive 95/46, 2 (a).

〔33〕 See Case C-101/01, Lindqvist, EU: C: 2003: 596, par 27, Case C-92/09 and C-93/09, Volker und Markus Schecke and Eifert, EU: C: 2010: 662; Case C-468/10 and C 469/10, ASNEF, EU: C: 2011: 777, para. 27.

〔34〕 第29号工作小组曾经以四项关键词来界定某项信息是否属于个人信息，第一，任何信息；第二，相关；第三，已识别或可识别；第四，自然人。See Article 29 Working Party, Opinion 4/2007 on the Concept of Personal Data' (WP 136), https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf，最近访问时间[2018-12-09]。

〔35〕 《条例》第4条第1款。

〔36〕 《条例》重述第23条。

〔37〕 See Ronald Leenes, "Do they know me? Deconstructing Identifiability", *University of Ottawa Law and Technology Journa* 4 (1-2) 1 (2008), p. 135; Paul De Hert and Serge Gutwirth, "Regulating Profiling in a Democratic Constitutional State", in Mireille Hildebrandt and Serge Gutwirth (eds), (eds), *Profiling the European Citizen*, Dordrecht: Springer, 2008, pp. 272-293.

入个人信息的范畴，支持者和反对者各自提出了若干理由。[38]

（一）支持理由

支持者的理由归纳起来有如下几点。第一，用户行为信息本身就是识别个体的方式，通过行为来筛选个体，这本身就是一种“识别”。根据这种观点，网站对个体进行用户画像，向个体推送广告，本身就是一种筛选或识别个体的活动。传统对于识别的定义往往将识别等同于联系到个体的姓名或地址，但事实上，姓名本身只是识别的方式之一。在网络社会，姓名甚至不是最有效的识别方式，相比起姓名，通过 Cookie 等技术收集的用户行为信息更容易“识别”个体，更能对个体产生影响。[39]

第二，在大数据时代，人们常常可以轻易地通过用户匿名化的行为信息识别个体的姓名。《纽约时报》曾经通过美国在线网站公布的匿名搜索记录很快识别了具体的个体。[40] 学者指出，匿名化是一种神话，伴随着大数据时代的到来，传统匿名化的手段已经基本失败，技术专家可以轻易地实现匿名化个人信息的再识别或者去匿名化。[41]

第三，个人信息保护的要义不一定是侵犯传统意义上的隐私，还在于规制风险，[42] 而网站大规模收集消费者行为信息所隐含的许多风险与信息是否匿名无关。即使消费者的行为信息属于匿名信息，但此类信息一旦泄露，还是可能给公民个体带来很多风险。[43]

第四，未经用户同意与法律规制的用户画像与个性化推荐还可能导致“寒蝉效应”。[44] 当用户发现自己的信息有可能在不知情的情况下被收集，那么用户就可能放弃搜索与查询相关信息。用户可能会感到自己对自身信息如何被收集与利用丧失了控制与预期，对网络产生不信任情绪。因此，即使网站的某些行为不像传统隐私侵权那样侵犯了用户的安宁或独处，但也应当受到法律的约束。[45]

（二）反对理由

反对者的理由归纳起来有几点。第一，如果法律将匿名化的行为信息视为个人信息加以规制，既然匿名化的数据也将受到同等的法律约束，那么数据控制者可能会从减小成

---

〔38〕 本部分对于支持者与反对者的理由综述受到了有关文献的启发。See Frederik J. Zuiderveen Borgesius, “Singling Out People Without Knowing Their Names-Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation”, 32 *Computer Law & Security Review* 2 (2016).

〔39〕 See Brian Lesser, How to Use Data to Deliver the Right Ad to the Right Person at the Right Time, http://adage.com/article/digitalnext/data-deliver-ad-person-time/235734/, 最近访问时间 [2018-12-19]。

〔40〕 See Michael Barbarom and Tom Zeller, A Face Is Exposed for AOL Searcher No. 4417749, www.nytimes.com/2006/08/09/technology/09aol.html, 最近访问时间 [2018-12-19]。

〔41〕 See Paul Ohm, “Broken Promises of Privacy”, 57 *UCLA L. REV.* 1701 (2010).

〔42〕 从风险角度解读个人信息保护，参见丁晓东《什么是数据权利？——从欧洲〈一般数据保护条例〉看数据隐私的保护》，《华东政法大学学报》2018 年第 4 期，第 45-50 页。

〔43〕 See Solon Barocas and Helen Nissenbaum, “Big Data's End Run around Anonymity and Consent”, in Julia Lane (et. al.) (eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (London: Cambridge University Press, 2014), pp. 44-75.

〔44〕 See Aleecia McDonald & Lorrie F. Cranor, Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising, https://www.researchgate.net/publication/228237033_Beliefs_and_Behaviors_Internet_Users'_Understanding_of_Behavioral_Advertising, 最近访问时间 [2018-12-19]。

〔45〕 See Ryan Calo, “The Boundaries of Privacy Harm”, 3 *Indiana Law Journal* 86, 1131 (2011).

本的角度考虑放弃匿名化的努力。[46]

第二，将匿名化的行为信息纳入个人信息范围，对用户画像与个性化推荐进行法律规制，将妨碍社会的创新与网络经济的发展。网站对用户行为信息的收集可以为消费者提供更好的服务，可以使网站与广告公司进行更为有效的营销，减少商家与消费者之间的信息不对称。[47] 因此，用户画像与个性化推荐本质上是一种基于算法的正常商业活动。[48]

第三，如果将消费者的行为信息也纳入个人信息范围，会导致个人信息的范围变得非常宽泛，可能任何信息都有可能变为个人信息。[49] 而一旦如此，对真正需要保护的个人信息就可能会保护不足。毕竟，无论是企业还是公共机构，其保护个人信息的能力都是有限的，而且这些机构也都有对个人信息进行利用的需求。

（三）对支持与反对理由的再思考

考察支持者与反对者的理由，可以发现支持者的有些观点有相当说服力。支持者正确地指出，消费者的匿名化行为信息既可以挑出或筛选出不具有姓名的个体，也可以帮助某些主体识别出个人的姓名等可识别性信息。无论是从风险控制、满足消费者预期、消除“寒蝉效应”还是保护消费者的角度，都有必要采取一定的法律措施，对网站收集与利用用户的匿名化行为数据和对消费者进行用户画像的行为进行法律规制。

但有些反对理由也有很强的说服力。第二点反对理由正确地指出，对用户匿名行为信息的合理利用将有效地促进商业活动。从消费者的角度来看，个性化推荐可以帮助消费者更快地获取自己想要的产品，节省信息搜寻成本。从商家的角度来看，个性化推荐可以帮助企业更有效地利用企业资源。对于中小企业而言，这尤其重要。在互联网经济中，个性化推荐可以帮助小企业的产品有效地为消费者所知晓。如果没有个性化推荐，那么互联网平台的流量就可能长期为少数大型企业所占据，消费者所能接触到的广告或推荐就可能永远是一些大企业的产品。从这个角度来看，互联网经济对于用户匿名行为的合理使用其实可以真正地惠及商家和顾客。互联网企业对于用户匿名行为信息的不合理使用当然会引起消费者不信任，最终损害互联网经济，但法律对于这种不信任的规制应当是促进信任，而非因噎废食地禁止用户画像与个性化推荐。

此外，第三点反对理由也值得重视。[50] 将用户的匿名行为信息都纳入个人信息的范畴，固然有利于进一步保护用户权益，但这种扩张性解释却可能导致所有信息都变为个人信息的困境。而一旦个人信息的概念界定过宽，不仅不利于某些信息的合理收集与使用，

---

〔46〕 See Leslie Stevens, “The Proposed Data Protection Regulation and Its Potential Impact on Social Sciences Research in the UK”, 2 *European Data Protection Law Review* 97 (2015).

〔47〕 See Nick Stringer, IAB UK: Could “Pseudonymous Data” be the Compromise Where the Privacy Battle is Settled?, www.exchangewire.com/blog/2013/03/14/iab-uk-could-pseudonymous-data-be-the-compromise-where-the-privacy-battle-is-settled，最近访问时间 [2018-12-29]。

〔48〕 See Michal S. Gal & Niva Elkin-Koren, Algorithmic Consumers, 30 *Harv. J. of Law & Technology* 1 (2017).

〔49〕 联邦贸易委员会也承认，可识别的个人信息与不可识别的个人信息的界限变得愈来愈模糊。See FTC, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, pp. 18-19.

〔50〕 对该理由的异议，See Frederik J. Zuiderveen Borgesius, “Singling Out People Without Knowing Their Names-Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation”, 32 *Computer Law & Security Review* 2 (2016), pp. 38-39。

而且也可能导致个人信息保护相关资源分配不均的情形，导致真正需要保护的某些个人信息得不到充分的保护。在当前个人信息保护面临严峻挑战的背景下，这一点尤其突出。无论是在中国还是在欧美，个人信息保护都面临着执法力量不足、新技术新挑战层出不穷的问题。如果将用户画像的法律规制等同于个人信息保护，将用户匿名行为信息视为一般的个人信息保护问题，有可能导致监管的重心出现偏差。

四 对个人信息概念的反思

用户画像与匿名化的用户行为信息之所以成为争议点，这与个人信息的概念有关。全球的信息隐私法或数据隐私法的框架都以个人信息为核心，当某类信息属于个人信息时，对其的收集与处理就受法律的保护；当某类信息不属于个人信息时，对其的收集与处理就不受法律保护。〔51〕 但现实表明，个人信息与非个人信息的界限并非如想象的那样清晰，同时，这一二元划分的框架存在着一定的问题。

就个人信息与非个人信息的界分来说，个人信息的范围常常会随着时代与科技的变化而变化。在信息隐私法发展之初的 20 世纪六、七十年代，个人信息的范围曾经相对确定。在那个时期，政府或企业主要收集的是个人的档案类信息，即个人的姓名、肖像、地址等能够直接识别个人的信息。对于公民个人的行为信息，例如个人在商场中的购物习惯、消费偏好，政府或企业并没有大规模收集，也并未将它们纳入个人信息的范畴。但随着时代的变迁、网络与信息技术的发展，对公民行为信息的收集越来越多，越来越普遍，和公民个体相关的公开信息也越来越多。而悖论的是，信息越多，成为个人信息的信息种类也越多。因为信息越多，就越可能通过信息的分析与交叉比对识别具体个人。随着整个社会的信息以指数级别的速度增长，未来可能所有或大部分信息都会变成个人信息，很多之前被认为与个人无关的信息，都可能和其他信息建立相关性，指向一个特定的个体。〔52〕

在这种背景下，以个人信息/非个人信息的二元划分来设计相关法律与制度，就可能存在问题。一旦消费者的行为信息被列入个人信息，就可能导致企业匿名化信息动力不足、不能合理利用个人信息、法律保护资源分配不合理等问题，而一旦此类信息不被列入个人信息，又可能导致个人信息保护力度不够、用户知情权丧失、“寒蝉效应”等问题。

在本文看来，较为合理的解决方案是隐私法权威学者保罗·施瓦茨与丹尼尔·索洛夫所提出的“个人信息 2.0”的概念。二位学者首先指出了个人信息与非个人信息边界的模糊化，个人信息的范围常常会随着科技的变化而变化，因为场景变化而变化，因而以个人信息为基础保护公民的相关隐私权益，常常会面临上文所提到的种种问题。〔53〕 但他们

〔51〕 一个非常典型的例子是欧盟对于个人信息与非个人信息的立法。对于个人信息，欧盟形成了以《条例》为代表的法律规制，但对于非个人信息，欧盟则形成了以《非个人数据自由流动框架条例》为代表的法律规制。前者以严格保护为基本原则，后者则以自由流动为基本原则。参见姚佳《非个人数据自由流动条例》能振兴欧洲数字经济吗？http://www.sohu.com/a/329568872_257489，最近访问时间［2019－01－02］。

〔52〕 See Nadezhda Purtova, “The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law”, 10 *Law, Innovation and Technology* 1 (2018).

〔53〕 See Paul Schwartz & Daniel Solove, “The PII Problem: Privacy and a New Concept of Personally Identifiable Information”, 86 *N. Y. U. L. Q. Rev.* 1814, 1836－1848 (2011).

同时指出，如果彻底放弃个人信息的概念，完全通过成本—收益与风险预防的进路来保护个人信息，又可能造成整个信息隐私法框架的重构，无论是监管机构还是个人信息的收集者与处理者，可能都会面临无所适从的困境。[54] 他们提出，替代方案是设计一个“个人可识别信息2.0”的分类，并根据这种新的分类适用不同的规则。

具体来说，可识别个人信息分为三类：已识别个人的信息、可识别个人的信息、不可识别个人的信息。已识别个人的信息是指已经确定能从人群中识别出某个人的信息；可识别个人的信息是指可能根据这些信息或结合其他信息而识别某个人的信息；不可识别的信息则是不可能识别到某个人的信息。[55] 对于已识别个人的信息，应当要求信息的收集者与处理者严格遵守信息隐私法规定的一系列责任，不允许有例外；对于可识别个人信息，则应当根据其可能带来的风险，对信息收集者与处理者施加不同程度的责任。[56]

以信息隐私法的基石“公平信息实践”为例，如果相关信息属于已识别个人信息，那么个体应当有一系列完整的信息权利，信息收集者与处理者应当承担一系列责任：第一，个人信息使用限制；第二，个人信息收集限制；第三，个人信息披露限制；第四，个人信息质量原则；第五，个人的被通知权，访问权和更正权；第六，透明性；第七，个人信息安全保护。[57] 但如果相关信息属于可识别的个人信息，那么信息收集者与处理者应当承担部分责任，例如第四点、第六点和第七点。而对于有的责任，例如第五点，则不应当作为信息收集者与处理者的责任。

对于责任要求，二位学者给出的理由是，个人可识别信息首先可能给个人带来风险，因此，对个人可识别信息的收集与使用不能放任自流，必须要求信息的收集者与处理者承担个人信息质量保证与个人信息安全保护的责任。个人可识别信息的收集者与处理者应当评估被收集信息的潜在风险，建立起一套“跟踪－审查”的模型，对信息收集、储存、处理与流转建立全流程跟踪与保障的机制。[58] 其次，透明性的责任有利于加强消费者、信息收集者与处理者的个人信息保护意识，同时赋予消费者以一定的选择权。[59]

对于豁免的责任，二位学者给出的理由是，赋予个体以被通知权、访问权、更正权等权利首先会造成用户隐私泄露的风险。为了保障个体的此类权利，信息的收集者与处理者必须在个人与相关信息之间建立直接联系，以确保个体能够行使此类权利。但悖论的是，这种直接联系反而会造成个体被直接识别，从而对个体的信息隐私造成直接威胁。此外，由于此类信息并不能直接识别个体，为了满足此类权利要求，信息的收集者与处理者也需

---

〔54〕 See Paul Schwartz & Daniel Solove, “The PII Problem: Privacy and a New Concept of Personally Identifiable Information”, 86 *N. Y. U. L. Q. Rev.* 1814, 1865－1870 (2011).

〔55〕 See Paul Schwartz & Daniel Solove, “The PII Problem: Privacy and a New Concept of Personally Identifiable Information”, 86 *N. Y. U. L. Q. Rev.* 1814, 1877 (2011).

〔56〕 See Paul Schwartz & Daniel Solove, “The PII Problem: Privacy and a New Concept of Personally Identifiable Information”, 86 *N. Y. U. L. Q. Rev.* 1814, 1880 (2011).

〔57〕 See Daniel J. Solove & Paul M. Schwartz, Information Privacy Law, 3d ed., (Wolters Kluwer, 2009), p. 907.

〔58〕 See Paul Schwartz & Daniel Solove, “The PII Problem: Privacy and a New Concept of Personally Identifiable Information”, 86 *N. Y. U. L. Q. Rev.* 1814, 1883 (2011).

〔59〕 See Paul Schwartz & Daniel Solove, “The PII Problem: Privacy and a New Concept of Personally Identifiable Information”, 86 *N. Y. U. L. Q. Rev.* 1814, 1882 (2011).

要付出较大的成本与努力，这与此类信息可能带来的风险并不相称。[60]

总之，施瓦茨与索洛夫给出了较为中道的解决方案。这一解决方案既没有采取美国较为狭隘的个人信息定义，将匿名化的行为信息等信息排除在个人信息的范围之外，也没有采取欧洲较为宽泛的个人信息定义，将匿名化的行为信息和其他已识别个人的信息同等对待。他们将可识别个人信息视为一个单独的个人信息种类，并且提出了区别于已识别个人信息的特殊规制方式。

五 对规制框架的反思

通过比较法的分析、对正反理由的思辨和个人信息概念的反思，现在可以对本文第一部分所提出的技术合法性问题进行分析。在用户匿名行为信息的收集阶段、融合阶段与利用阶段，法律应当根据不同技术所涉及的不同风险采取不同的规制进路。

在信息收集阶段，应当要求信息收集符合透明性要求。信息的收集应当符合消费者的合理预期，应当给予消费者以拒绝信息收集的权利，避免秘密和不合理的收集。[61] 这是因为，尽管用户的匿名行为信息不能直接定位或识别具体个人，但此类信息的收集、聚合与利用仍然可能给人带来相应的风险。在这种前提下，保障消费者的知情权与选择权，仍然有其必要性。这些权利不仅可以为消费者提供一定程度的警示与选择自由，而且也可以减少消费者被冒犯的可能，帮助互联网企业赢得消费者更多的信任。

具体就本文在第一部分提到的信息收集方式而言，利用 Cookie 进行的信息收集应当被允许，因为一般的网站浏览器都提供了 Cookie 的删除选项，而且 Cookie 技术也已经为广大消费者所熟知。这里可能需要注意的是，如果是第三方平台利用 Cookie 技术收集用户行为信息，此时用户访问的相关网站应该在网站隐私政策中进行明确的告知，确保消费者意识到，存在第三方收集用户消费行为信息。

而对于利用 Flash Cookie、Ever Cookie、Fingerprinting 技术收集用户行为信息，则应当要求互联网企业对用户进行更为明确的告知，并且只有在用户明确选择同意加入的前提下，这几种技术才能被法律允许。[62] 这是因为，这几种技术使得用户很难或无法拒绝网站对其信息的收集，即使用户删除了网站浏览器自带的 HTTP Cookie，网站也仍然可以继续收集其用户行为信息。Fingerprinting 技术虽然未在用户电脑中隐藏或不断复制Cookie，但由于其比对功能也很容易通过关键信息的比对来识别特定电脑，因此也应当保持透明性，应当获得用户的明确授权。这里尤其需要强调的是 Ever Cookie 技术，由于 Ever Cookie 技术在一定程度上剥夺了用户的删除权，而且具有非常隐蔽的性质，因此更应当获取用户明确无误的同意。除非获取用户明确无误的同意，否则不应当允许企业运用此种技术

---

〔60〕 See Paul Schwartz & Daniel Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information", 86 *N. Y. U. L. Q. Rev.* 1814, 1880 (2011).

〔61〕 类似的观点，参见朱芸阳《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》，《社会科学》2016 年第 1 期，第 105 - 109 页。

〔62〕 参见万方《隐私政策中的告知同意原则及其异化》，《法律科学》2019 年第 2 期，第 61 - 68 页。

来收集用户匿名行为信息。[63]

在信息融合阶段，应当从总体上允许企业利用其合法收集到的信息与数据进行用户画像。毕竟，信息与数据的融合与利用是互联网与大数据的本质所在，允许此类用户行为信息与数据的融合与“化学反应”，可以给商家和消费者带来双赢。在这一阶段所需要的问题是，数据的融合汇聚应当注意防范相应的风险，进行数据融合的数据管理平台应当承担数据的安全保障义务。[64] 因为此类数据一旦泄露或被不法分子利用，就可能造成重大社会负面效应。

在信息利用阶段，对于用户匿名行为信息的利用应当遵循上文提到的风险规制原则，即根据用户匿名行为信息的潜在风险不同向信息处理者施加不同的责任。相关网站可以利用用户的消费偏好与习惯进行个性化推荐，但不应利用敏感类信息进行个性化推荐。在朱烨案中，虽然终审判决认定百度的个性化推荐合法，但随着网络安全法的生效以及个人信息保护法的起草，未来应当禁止利用此类敏感信息进行用户画像与个性化推荐。不同于其他匿名行为信息，此类敏感信息可能给个体带来很多困扰。因此即使个人授权网站收集其所有行为信息，也应当限制网站对此类敏感信息进行个性化推送。[65]

总之，用户画像与个性化推荐的法律规制框架可以借鉴与适当沿用个人信息法律保护的框架。法律应当将用户匿名行为信息纳入个人信息的范围，但应当将此类信息视为一个单独的类别——可识别的个人信息。法律应当对此类信息采取基于标准的规制方式，对其进行风险评估。当收集与处理此类信息的风险较高时，应当进行较为严格的法律规制，要求互联网企业遵循个人信息保护的相关责任；当收集与处理此类信息的风险较低时，则应当进行相对宽松的法律规制，要求信息的收集者与处理者承担部分责任。

六 结 语

用户画像与个性化推荐是伴随互联网经济发展而兴起的重要商业模式，在这一过程中，新的技术问题与法律问题层出不穷。尤其是通过个人信息保护的视角来看待用户画像与个性化推荐问题，可以发现互联网企业对于用户匿名行为信息的收集、融合与利用存在很多争议。何种技术应当被允许？法律应当采取何种框架应对相应问题？这需要同时从技术与法律两个方向进行深入分析。

本文认为，应对用户画像与个性化推荐提出的挑战，应当对现有的法律规制框架进行反思。法律既不能直接将匿名化的用户行为信息视为非个人信息，也不能将此类信息等同于可直接识别的个人信息。对于用户画像与个性化推荐，应当在赋予消费者知情权和

---

〔63〕 技术并非中立，在个人信息保护中，技术设计应当符合信息伦理，参见郑志峰《通过设计的个人信息保护》，《华东政法大学学报》2018 年第 6 期。

〔64〕 关于网络平台的安全保障义务，参见梅夏英、杨晓娜《网络服务提供者信息安全保障义务的公共性基础》，《烟台大学学报(哲学社会科学版)》2014 年第 6 期，第 14 - 21 页。

〔65〕 毕竟，个人并不一定能够对自己的隐私利益做出合理的判断。参见 Daniel Solove, “Privacy Self-Management and the Consent Dilemma”, 26 *Harv. L. Rev.* 1880 (2013)；丁晓东《个人信息私法保护的困境与出路》，《法学研究》2018 年第 6 期，第 194 - 206 页。

拒绝权的同时，更多要求企业承担相应的治理责任与信息伦理，真正保证用户画像与个性化推荐是为了为消费者提供更好的服务，符合消费者在具体场景中的合理预期与信息的合理利用。从这种规制框架出发，[66] 既可以对现有的各种技术问题进行分析与反思，也可以为未来新出现的技术手段与新问题提供理论框架与规制基础。

[本文为作者主持的 2018 年度国家社会科学基金一般项目“大数据背景下的个人信息保护与企业数据权属研究”(18BFX198) 的研究成果。]

[Abstract] User profiling and personalized recommendation have become more and more common in the network society and posed challenge to the protection of personal information. An analysis shows that there are many irregularities in the collection of users' anonymous behavior information. On the one hand, users' anonymous behavior information should be included in the scope of personal information to ensure users' right to know or object profiling and personalized recommendation. On the other hand, users' anonymous behavior information should be treated differently from identified personal information and be protected by a special mechanism. In the regulation of the collection and use of information in user profiling and personalized recommendation, enterprises should be required to assume more governance responsibilities to ensure the quality and security of users' information. At the stage of gathering the user anonymous behavior information, enterprises should be allowed to collect information with the explicit consent or reasonable expectation of users; at the stage of information aggregation and user profiling, they should be required to undertake corresponding data security obligations; and at the stage of information utilization and personalized recommendation, enterprises should be required to pay attention to relevant ethical norms and avoid using user sensitive information to facilitate personalized recommendation. Generally speaking, enterprises should adopt a risk regulation path based on standards, rather than rules, and avoid applying the general legal framework of personal information protection in the collection, aggregation and utilization of users' anonymous behavior information.

(责任编辑：田 夫)

[66] 从个人信息保护的责任模式来说，这意味着应当要求企业承担更多的治理责任与信托责任。参见周汉华《探索激励相容的个人数据治理之道——中国个人信息保护法的立法方向》，《法学研究》2018 年第 2 期，第 3 - 23 页；Jack M. Balkin, "Information Fiduciaries and the First Amendment", 49 *U. C. DAVIS L. REV.* 1183。