东方法学
Oriental Law
ISSN 1674-4039,CN 31-2008/D

《东方法学》网络首发论文

题目：知情同意原则在信息采集中的适用与规则构建
作者：郑佳宁
DOI：10.19404/j.cnki.dffx.20200220.003
网络首发日期：2020-02-21
引用格式：郑佳宁．知情同意原则在信息采集中的适用与规则构建．东方法学.
https://doi.org/10.19404/j.cnki.dffx.20200220.003

DOI：10.19404/j.cnki.dffx.20200220.003 网络首发时间：2020-02-21 16:44:08
网络首发地址：http://kns.cnki.net/kcms/detail/31.2008.d.20200220.1234.006.html

知情同意原则在信息采集中的适用与规则构建

郑佳宁*

内容摘要：用户的知情同意作为企业采集用户行为信息应遵守的一项原则，是用户行为信息采集的合法性基础。在信息采集中的选择与参与机制中，我国宜采择入为主的知情同意规则设计。在其必备前提——告知环节，针对信息采集行为的主体、行为信息的类别和使用目的、采集后的处理行为和用户行为信息流向的第三方等方面，均应履行告知义务。对用以进行行为化定位等特殊用途，还应进行专门披露。在用户同意规范制度的设计上，用户同意类型需要进一步区分；同意的有效形式应该更加审慎；同时，对用户同意外的其他采集合法性基础应进行明确。

关键词：数据信息 信息采集 合法性基础 知情同意 择入机制 择出机制

用户行为信息，可被定义为用户使用互联网企业所提供的服务或产品时，伴随使用服务之行为而生成的一系列数据信息。具言之，包括用户通过鼠标、键盘、手机、智能手环、语音识别设备、智能化触控设备等信息输入端硬件设备访问浏览器、网页或其他设备界面，以进行诸如点开视窗、滑动浏览、输入信息、关键词搜索、发表评论、上传图片、提供定位、在线交易、下达指令、个性化设置等具体行为。用户行为信息的生成既可能是用户在使用互联网产品或服务时主动、有意识地提供，也可能是用户使用在线服务的行为轨迹，在无意识状态下不知不觉地被互联网企业的自动化信息抓取工具所采集而生成。用户行为信息能够直接反映用户个人在信息世界中的行为概况，经分析后进行的数据画像与基于画像结

* 中国政法大学民商经济法学院教授、博士生导师。

本文系 2019 年教育部规划基金项目“数据财产私法规制体系的重塑研究”（项目批准号：19YJA820057）的阶段性研究成果；2018 年中国政法大学青年教师学术创新团队资助项目(项目批准号:18CXTD08)。

果的定向广告推送更关乎用户的个人隐私与人格自由。因此，用户对行为信息似乎理所应当地应拥有某种控制权利——不管这项权利是被视为独立的自决权，还是被认作个人隐私空间在数据信息视域中的自然延伸。无论如何，均需承认的是，用户才是行为信息商业化流转的初始源头。也正基于此，各国立法几乎不约而同地将征求用户的知情同意作为企业采集用户个人信息时应遵守的一项原则。

一、知情同意——用户行为信息采集的合法性基础

同意原则根植于契约自治理论之中。在行为信息采集的场景下，不同的互联网企业与用户之间均存在着内容近似的合同关系，而企业对用户行为信息的采集恰是用户与企业所订立合同的内容之一。自动化、信息化的网络平台虽使得借助互联网技术订立的合同在细节上与传统意义上的合同有所不同——如我国《电子商务法》即规定用户“提交订单”之行为可以被视为缔结电子商务合同的承诺行为。[1]互联网上用户与企业之间的种种交易当属合同法规制范畴，用户行为信息的采集自然也在其列，其法理前提理应是由用户与企业间订立的诸如“服务协议”“软件使用许可协议”甚至“隐私协议”等一系列协议而构建的合同关系。这种互联网企业与用户间就互联网产品使用与互联网服务而订立的系列约定，因其权利义务关系的复杂且不断发展的现状而暂未在合同法中取得有名化地位，[2]但亦在基本的对待给付上拥有共性，可资分析。

具言之，以合同理论的视角来看，互联网服务合同的对待给付一面是企业所提供的诸多网络产品或服务，另一面则相应地是用户为企业所贡献的价值。后者既可能体现为直接的现金给付，如用户所支付的注册费、会员费抑或直接为产品

[1] 参见《中华人民共和国电子商务法》第 49 条。

[2] 从法律本质上来看，上述协议属于服务合同的范畴。在民法典编纂的大背景下，有关服务合同的有名化实现路径正成为学界热议的话题。就研究思路而言，既包括服务合同入“典”的顶层设计研究，也包括针对某一特定类型服务合同典型化的具体探讨。相关文献，参见周江洪：《作为典型合同之服务合同的未来——再论服务合同典型化之必要性和可行性》，载《武汉大学学报（哲学社会科学版）》2020 年第 1 期；郑佳宁：《快递服务合同典型化的立法表达与实现路径》，载《法学家》2019 年第 1 期。

付出之费用。与此同时，也可能是间接的、潜在的价值让渡，其典型正是企业对用户进行的行为信息采集。这些用户行为信息正如同隐藏的黄金矿脉，具有极高的价值回报潜力，将为企业带来高额的收益——与用户相关的数据信息已经被人们视作一种价值丰富的商品，只需极少的数据挖掘成本投入，就可能收获巨额的利润回报。[3]应特别说明的是，商业实践中用户所享受的免费互联网服务，并非毫无对价，往往是以用户对行为信息采集之容忍为代价。正是因基于用户行为信息的定向广告推送所带来的巨大利润，以搜索引擎网站为首的众多互联网企业方能向用户提供“免费”的服务或产品。当然，在一些用户为互联网产品或服务付费的场景下，用户行为信息本身也许并不单独地构成合同的对待给付。但无论如何，在当今以用户需求为导向的互联网商业模式下，采集用户行为信息已经与互联网服务的个性化提供模式密不可分，互联网企业很难对唾手可得的用户数据信息资源做到视而不见、过而不取。

无论企业对用户行为信息的采集是互联网服务合同订立的本质目的，还是互联网服务提供所必然伴生的副产品，行为信息的采集均匿于用户与企业间合同法律关系之中。那么，用户对于采集其行为信息的同意在这一过程中又处于何种位置呢？依循合同法理论的思路，用户当然地享有缔约之自由。因此，当且仅当用户做出同意之意思表示，自愿进入包含行为信息采集内容的契约关系时，企业对用户行为信息的采集方才具备了正当化基础。事实上，用户同意所展示出的正当化采集行为之法律效力，并非仅停留在合同法理论中契约自由的层面。用户自行选择与企业建立以行为信息采集为内容的法律关系，更蕴含了作为私法筑基之石的私人自治原则之价值。就行为信息采集的情境而言，同意是用户个人就信息进行自决的意思表示，故而，将用户同意作为企业采集用户行为信息的合法化基础无疑是对私人自治的尊重与保护。

诚如前论，征询用户的同意正是私人自治原则在涵盖信息采集内容的互联网服务合同情境中的应有之义，亦是判定企业能否合法采集用户行为信息的关键节

[3] John T. Soma, J. Zachary Courson& John Cadkin, *Corporate Privacy Trend: The Value of Personally Identifiable Information (PII) Equals the Value of Financial Assets*, 15 Richmond Journal of Law and Technology 1, 9-10 (2008).

点。应补充说明的是，用户的同意并非径直作出，同意与知情这一前提牢牢绑定，难以分离。如从契约自由的角度出发，个人自愿创设契约关系并受其约束的当然前提便是清楚地知晓该契约的权利、义务与责任内容，任何合同的当事人都不会也不应受到未知条款的约束，这是合同法中不言自明的原理。从经济学意义上而言，个人在信息不对称的前提下对自身事务的安排当然也不再具有效率上的优先性。由此可知，用户的知情是用户对采集行为作出同意表示的必然逻辑前提，欠缺知情的同意无疑将存有瑕疵。

用户的知情同意是用户作为个体就本人事务自决之行为，那么法律何以如此关注采集的同意这一私人自治之环节，甚至专门就其内容和形式作出规定呢？背后的原因在于，私人自治只有在各有关交易主体之间在经济、社会等诸多方面力量均衡的条件下才能得以实现。在当前的技术背景下，诸多因素共同决定了，用户在与企业就行为信息的采集的潜在角力过程中，几乎必然落于下风。因而，用户很难真正地在知情和理解的基础上自由地行使对于自身行为信息采集和后续处理过程的自决权利。其中，最重要的影响因素如下：

其一，在经济上占具强势地位的互联网企业得以通过对隐私政策、用户界面的刻意设计，使用户难以形成对行为信息采集范围、方式、用途的正确认知。隐私政策设计上，企业往往会向用户提供篇幅冗长、排版混乱、结构复杂且文字诘诎聱牙的隐私相关条款，使得用户难以清晰地知悉其行为信息经采集后可能伴随的隐私风险。界面安排上，企业可以轻易地通过技术手段，在界面上插设误导性链接、无法返回的按键、无必要且复杂的表格，甚至刻意遮盖有关内容的弹窗，以在用户浏览信息采集相关的隐私警示条款或作出同意表示时进行干扰或影响。由此，复杂的隐私政策使得用户无从确切地认识到行为信息采集的过程与潜在风险，不友好的界面则使得用户即便对企业的采集行为心存顾虑，亦难以作出“不同意”的拒绝表示。

其二，信息的过载和不足同时存在，导致用户知情大打折扣。一方面，在采集前的知情环节中，用户面临着大量数据信息的不间断轰炸。宏观上，当前数据主导的商业模式使得用户行为信息的采集已经成为了互联网企业生存和发展的

必然手段，用户无时无刻不面对着企业请求采集其信息的请求和附带的告知条款。微观上，正如前述，形形色色隐私政策都具有篇幅冗长、信息繁多的共通之处。故而，有助于用户作出决定的少数有效信息被刻意混杂在海量无效、无关信息之中，信息筛选无异于大海捞针。如此畸高的信息提炼成本用户当然无力承担，知情流程自然将流于形式。因而，所接收信息总量过载并不意味着用户拥有充足的信息来源，反而，用户还同时面临着信息不对称所导致的有效信息不足。

其三，用户固有的认知局限和行为偏差，加之智能化处理的黑箱效应，使得用户信息自决的结果难以被准确预料。抛开信息不对称的外部影响，理性的局限往往会使得人类陷入诸多偏差之中，最终将使用户很难真正认识到用户行为信息经采集、处理后可能对其隐私等人格权益带来的不良影响，或即便认识到了风险，亦会因为对未来利益的忽视、过于乐观和感性，忽略而容忍存在不可控风险的采集和处理行为，因而作出于己不利的信息自决。除此之外，即便是企业，亦无法完全掌控数据信息经自动化处理后可能带来的嗣后风险，因为大多的处理行为已经在人工智能的“黑盒”中进行，其极高的运算速度和复杂的程式设计无疑加剧了结果的不可预料性。

二、择入机制与择出机制的讨论——知情同意原则的实践抑或背离

有鉴于私人自治价值的局限，尽管各国几乎均对信息采集同意这一私人自治环节进行了一定规则干预，并将知情同意提高到了信息采集原则之高度。然而，知情同意原则在各国立法中的应用方式却不尽相同，与保护个人信息和促进行为信息商业化利用的实效亦是大相径庭。其中一项显著的区别在于：是否将主动征求用户的知情同意作为一项必须的采集正当化前提；还是可凭借用户的不作为表现径直推定用户的知情同意，转而赋予用户不同意继续被采集时的拒绝权利——这项区别标准正是知情同意的择入机制与择出机制划分之关键。

择入机制与择出机制的提法围绕着用户在采集中的选择与参与展开。企业虽然是用户行为信息的采集者，但用户行为信息的根本源头是用户本身，有关择入

机制与择出机制的探讨正体现了用户在行为信息采集中不容忽视的角色。质言之，用户对采集过程的参与有两种基本的路径：

一是择入机制。即用户主动通过肯定性的表示，选择参与行为信息的采集进程。在择入机制路径下，用户行为信息的采集前提是征求用户的许可，否则，采集的进行将欠缺合法性基础。

二是择出机制。即用户在采集过程中拥有选择退出的权利。企业对用户行为信息的采集无须征得用户的事前同意即可开展，用户所能做的选择仅仅是采取行动退出采集流程。应予以明确的是，择出机制中，所谓的用户事前同意是被推定的“默示同意”，用户所切实拥有的权利只是被采集后的“不同意”，即拒绝的权利。择入机制与择出机制的立法选择背后体现了各国在平衡用户与企业利益时不同的政策考量。择入机制在设计上显然更为偏重用户对相关个人信息的掌控与自决，强调非经明示同意，企业不可擅自对用户的行为信息进行任何方式的采集；而择出机制则反而更为偏重用户行为信息的商业化利用效率，企业对于采集便利化的诉求在这一机制下更易实现。

从当前全球的立法情况来看，欧盟由《一般数据保护条例》为统领的用户个人信息保护规则采择入机制作为主要的采集范式。该条例将用户的知情同意作为采集合法最重要的前置条件，并将采集同意的证明责任置于数据控制者，即企业一方。[4]故而，欧盟以择入为主的采集机制设计更倾向于保护用户就个人信息所拥有的权益。美国的用户知情同意机制则以择出式为主。联邦立法上，按照《电信法案》的规定，互联网内容提供商在为使用或分享采集敏感的用户个人信息时，应当遵照择入机制，取得用户的同意；而在采集内容更为丰富的非敏感个人信息时，则只需采用择出规则即可。[5]值得注意的是，2016 年美国 FCC 曾就加强宽带和其他电信运营商在采集用户个人信息时披露相关信息且征求用户同意的义务方面颁布了命令，要求互联网服务提供商也应适用并遵照上述电信法案的规定。

[4] Article 6, Article 7, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[5] TELECOMMUNICATIONS ACT OF 1996, 47 USCA § 222.

不过，该命令在 2017 年于立法程序上遭到了美国国会的否决。从该命令受挫之结果可以推断出，美国联邦层面在用户信息采集上的政策导向显然以企业的商业化利用为先。在州立法层面上，即便是当前最为严格的 2018 年《加州消费者隐私法案》，从其规定亦足以看出择出机制的主导地位——企业采集用户个人信息时并无征求同意之义务。企业可先行采集用户的行为信息，只是在采集行为发生时或发生前，应对用户进行相应的信息披露。[6]可见，美国以择出机制为主的采集机制设计对企业采集用户行为信息的效率和便利更为看重。

倘若以规则适用的视角切入，择入机制和择出机制的区别即体现在，当用户本身并未对行为信息的采集作出肯定的意思表示时，是否存在一项默认用户对此表示同意的缺省规则。在择入机制下，欠缺用户的明确同意即意味着默认的规则是用户行为信息采集的禁止，而在择出机制下，只要用户未曾通过某种流程表示反对，则默认用户行为信息可被合法采集。事实上，在用户行为信息采集这一过程中，缺省规则[7]的设置颇为必要：一方面，缺省规则有着强制性规则所不具有的灵活性，它并不对身处商业实践中的用户或企业施加任何法律上的强制力，而仅仅为不完备的私人约定提供兜底的补缺规则。如此一来，用户行为信息采集情境的多样性得以被顾及，进而促进了用户行为信息的商业化利用。另一方面，缺省规则具有很强的规则粘性。事实上，相当比例的当事人在实际交易时会遵从缺省规则的内容而不是耗费额外的缔约成本，进行另行约定，这可归因于缺省规则对缔约协商等交易成本的大幅减省之效。正因如此，用户行为信息采集统一的缺省规则必须审慎设计。

笔者认为，基于下述两点理由，我国宜采择入机制为主的知情同意的缺省规则：

其一，从缺省规则的法理来看，缺省规则的一大功能，是缓释缔约双方在信息地位上的不对称所引发的不完全契约问题。就企业对用户行为信息的采集而言，

[6] Article 1798.100. (a), Article 1798.100. (b), California Consumer Privacy Act of 2018.

[7] 缺省规则，是指未被约定所排除即可推定适用的补充性规则。参见黄辉：《对公司法合同进路的反思》，载《法学》2017 年第 4 期。

企业作为采集主体掌握着包含采集方法、目的、后续处理与风险在内的大多数相关信息，当然地占据着信息高地。尽管将缔约相关信息尽数披露给用户能解决双方在信息上的不匹配，有利于整体缔约收益的提升，但企业作为逐利的理性人，显然会更愿意隐瞒部分信息，以追求己方在缔约过程中的最优位置——与其做大蛋糕，不如利用信息之不对称为己方争取更多的利益分配。因而，为缓解用户信息采集过程中企业与用户间的信息不对称，缺省规则的安排就自然应当偏向处在信息劣势的用户一方，也即以须取得用户事前知情同意的择入机制为默认规则。如此一来，立法者将能借助择入机制的规则粘性改善用户在行为信息采集过程中的信息劣势，消减企业的信息寻租之行为，从整体上促进用户行为信息采集的社会效益产出。[8]

其二，在某些欧洲学者看来，“先同意、后采集”的择入机制无疑是对知情同意原则的根本贯彻；反之，择出机制则是“挂羊头卖狗肉”，以“默示同意”为幌子，实际则背离了知情同意原则的基本理念。盖因从本质上看，这一择出机制并没有为用户提供做出同意的任何空间。[9]择出机制的逻辑下，用户的沉默，或者访问网站、点开手机 APP 等不相干行为，将被企业视作对行为信息采集的“默示同意”。故而，往往在用户登陆网页、打开 APP 或其他智能设备的同时，企业即已经基于此“默示同意”，使用 Cookies 等自动化工具开展采集，用户对此无置喙余地，所拥有的权利仅仅是退出与拒绝。况且在择出机制下，即便是退出与拒绝权利的行使亦并不轻松，往往需要经由一系列程序方能成功退出，故用户对应用择出机制并不欢迎。故而，择出机制在欧洲的实践应用容易受到司法的否认。1995 年英国的 Linguaphone Institute Ltd 诉 Data Protection Registrar 一案中，英国数据保护法庭即否认了该案件中 Linguaphone 公司向用户所提供的择出式采集同意征集方式的有效性。该案中，Linguaphone 公司仅仅在订单界面表格的尾部，用极小的字号，给用户提供了表示拒绝个人信息采集的退出弹窗框。虽然，法庭未对择出机制作出普遍意义上的论断，但至少认为本案中 Linguaphone 公司采用

[8] Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 Yale Law Journal 87, 94 (1989).

[9] Eleni Kosta, *Consent in European Data Protection Law*, Martinus Nijhoff Publishers, 2013, p.188-189.

的方式无法获得用户对采集的有效同意。[10]

三、告知——知情同意原则的必备前提

知情同意原则下，企业应负告知义务已广为立法与实务界所认可。然而，告知的内容和方式在各国却尚无统一的标准。企业往往通过行文冗长、信息混杂、用词艰涩的隐私政策等方式向用户告知其行为信息的采集情况，[11]知情环节时常沦为形式，用户基于不充分知情所作同意在效力上亦饱受争议。可以说，知情前提上存在的瑕疵，很大程度上影响了知情同意原则理论践行的有效性。因此，知情同意原则中的告知环节应达到下列标准：

第一，采集告知的表现形式应当是清晰且显著的。诚如前文所述，当前，载有告知内容的隐私政策、隐私协议、信息共享协议等文件在用语上青睐专业词汇，致整体行文生涩难懂；在篇幅上好长篇大论，似把告知文稿当作免责协议，欲将所有相关内容融于一体；在结构设计上复杂混乱，轻重失调，将重要信息混藏于海量无关信息之中。[12]这类采集告知使得用户难以在真正知情的前提下作出同意，企业与用户也就无法在行为信息的采集上达成合意。就此，立法者呼吁企业加强隐私政策的透明度，有学者亦对采集告知环节信息透明度的增强提出了如下建议：其一，用语上避免采用生涩的法律或计算机技术专业术语，转而使用平实且直白的语言进行表达。在向用户告知采集相关信息的环节中，专业的用语非但不能有利于表达，反而将使不具有专业素养的用户难以理解有关内容。其二，告知形式应当显著，这意味着记录告知内容的隐私政策等形式须出现在用户可能看见的界

[10] Linguaphone Institute Ltd v Data Protection Registrar [1995] UKIT DA94_31491 (14 July 1995).

[11] 例如，2019 年 12 月 11 日生效的最新版本的淘宝网《隐私权政策》包括九个部分，高达 1.5 万余字，载淘宝官方网站 https://terms.alicdn.com/legal-agreement/terms/suit_bu1_taobao/suit_bu1_taobao201703241622_61002.html，2020 年 1 月 12 日访问。又如，2019 年 12 月 9 日生效的最新版本的《京东隐私政策》包括八个部分，多达 1.6 万余字，载京东官方网 https://about.jd.com/privacy/，2020 年 1 月 12 日访问。再如，《百度隐私政策总则》包括十部分，共计 1 万余字，载百度官方网站 http://xueshu.baidu.com.cn/duty/yinsiquan-policy.html，2020 年 1 月 12 日访问。

[12] Corey Ciocchetti, *Just Click Submit: The Collection, Dissemination, and Tagging of Personally Identifying Information*, 10 Vanderbilt Journal of Entertainment & Technology Law 553, 586-589 (2008).

面之中，且这种看见的可能性至少应当是合理的。譬如，在用户需要以电子签名等方式提交采集同意之确认的界面上，既应简明扼要地显示将采集信息的类别、用途、采集方式、第三方等要点信息，又应在该界面上提供显著的链接，以便用户查看完整的隐私协议内容。[13]

第二，采集告知的程度应当深入揭示采集行为信息的方法与目的，并适当提示行为信息经采集处理后的预备用途与潜在风险。有些企业以复杂且模糊的形式向用户告知情况，其目的在于刻意隐藏或回避信息采集后的处理和应用方式，以免用户意识到风险而拒绝同意。目前，采集告知所缺失的典型内容，并非通过积极或消极方式所采集的行为信息本身之类别，而是这些被采集行为信息的后续处理过程，后者往往能够在某种程度上改变行为信息的价值和其可能带来的风险。因此，采集告知内容需要得到清晰化、分层化的处理。企业就行为信息采集所进行的告知不应当将确定的事实与可能的风险混为一谈，不能对无法确知的后果进行武断的保证，当然更不能刻意地模糊可能对用户带来隐私风险的后续处理过程。采集的告知在内容上应当是渐进的，具备一定的层次。第一层次的告知应当在采集行为本身的层面进行。企业应当以清晰且平实的方式向用户说明采集主体、被采集行为信息的属性和内容，以及所使用自动化采集工具的基本功能等情况。第二层次的告知则不应仅停留在采集环节本身，而应深入采集后自动化处理的层面，将人工智能和算法对行为信息后续利用环节带来的不确定性和潜在风险毫无保留地充分告知用户。

具言之，企业至少应加强下述方面信息的告知：

首先，采集行为的主体。主体是合同缔结时必须显现的内容，不知主体，则用户无法凭借外部信息对采集者的信息安全把控能力作出预判。譬如，欧盟即要求隐私声明等告知文件，应明确展示数据控制者的身份。[14]欧盟语境下的数据控

[13] Patrick Myers, *Protecting Personal Information: Achieving a Balance Between User Privacy and Behavioral Targeting*, 49 University of Michigan Journal of Law Reform 717, 742-743 (2016).

[14] Article 13(1)(a), Article 14(1)(a), REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

制者，实际上仅指向采集主体中单独或共同决定个人数据采集、处理目的与方式的实体。[15]笔者认为，披露控制者固然是必须之举，其余参与、辅助或者能直接经采集而获取用户行为信息的主体亦应被定义为采集者，并在告知中如实披露。如采集用户信息的企业可能隶属于某一集团，则其控制者既可能为母公司，又可能为承担某一浏览器、网页或手机 APP 项目的特定子公司。此时无须踟蹰于判断控制者之身份，参与采集之采集者均应得到披露，且其在采集中的不同角色担当亦应载明，以助用户对采集主体形成正确认知。类似的做法亦应适用于同一界面多采集主体的情境，与因收购等控制权变动而发生主体性变化的情形。之所以对采集主体的告知作出堪称严苛的要求，是因为用户作出同意采集的决定在一定程度上是基于对所有采集者的商誉、隐私保护政策和措施的信赖。

其次，行为信息的类别和使用目的。行为信息是采集行为的对象，当然地居于应被告知内容的核心地位。用户同意的具体性要求，是指就个人信息处理的同意，必须针对具体的情形明确作出。从合同理论的基本原理出发，意思表示必须是明确且具体的，概括的同意显然不符合法理之要求。具体的同意自然需要相应的具体化告知，以消除用户与企业间的信息不对称。一是要明确欲采集信息的类别。即企业应对目标信息以合理的标准进行分类，向用户告知具体的类别。二是要明确采集和使用用户行为信息的目的，这既包括通用目的，也包括特殊目的。美国加州《消费者隐私法案》也明确要求企业对所采集消费者信息的特定使用目的进行告知。[16]采集和使用行为信息的目的应事前即被明确告知，行为信息不得为未被告知的目的而使用。

再次，采集后的处理行为。企业的告知应如实阐述行为信息分析的深度，着力于消除采集后续处理行为中的信息不对称现象。企业对信息的处理手法决定了数据挖掘所能达到的深度。Web 3.0 时代下，各源头信息的相互融合已成为大势。特别需要注意的是，互联网企业完全有能力，将通过电脑、手机客户端、智能家

[15] Article 4(7), REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[16] Article 1798.100. (b), California Consumer Privacy Act of 2018.

居设备等多源头采集的用户行为信息融合一体，如 Apple 集团同时为电脑、手机、家居设备提供软件服务，并通过 Siri 等跨平台项目同时采集用户信息。这种多传感器信息融合（Multi-sensor Information Fusion, MSIF）的信息采集和处理方式很可能使得诸多原本十分简单的行为信息在无数次的智能化融合后，成为能够反映更为复杂现象的重要信息。此外，多传感器信息融合处理还可能由人工智能算法进行，其结果无法被完全预测，故原本与隐私等人格权益无涉的行为信息经融合后亦可能变得更为敏感。因而，倘若企业将可能同时通过多种设备采集用户行为信息，应当对此进行清晰的特别告知。

又次，告知用户行为信息流向的第三方。即便是经企业采集、处理后，用户行为信息亦不同于企业制造的产品，不可为企业所自行交易、自由处置。这是因为只要未经匿名化这一特殊处理环节，行为信息就仍与用户个体的人格紧密关联，企业只有在满足个人信息保护的基本条件后，才能对采集、处理后的信息具有完全的支配权，充分实现经营者信息的财产价值与个人人格尊严的和平共处。[17]因而，行为信息的后续处置与流转同样不能绕开用户，应在征得用户同意后方可为之。出于商业利益最大化的考量，互联网企业与第三方之间的数据流通被刻意地隐瞒，利益相关者之外的知情者寥寥无几。这也使得实际掌握了用户行为信息的众多数据中间商隐匿在社会视线和规范底线之外。这些身份晦暗的数据中间商专营数据处理与分析，采集到用户行为信息的企业将信息传输给数据中间商，后者将其进行格式转化、内容萃取或者行为化定位等处理，再将其打包转卖。数据中间商因而成为用户行为信息商业化流转过程中必经环节。这一灰色交易链条显然威胁到了用户个人信息的安全，因而，是否有第三方参与处理或受让用户信息，理应在告知内容中占有一席之地，用户需在充分知情的前提下决定自身行为信息的进一步去向。

最后，当用户行为信息被进一步处理且用以进行行为化定位、个性化推荐、自动化决策等用途时，企业应当告知用户行为化处理之事实、原因、基本算法逻

[17] 参见郑佳宁：《经营者信息的财产权保护》，载《政法论坛》2016 年第 3 期。

辑、预期分析后果与可能产生的风险。[18]行为化定位处理的核心做法是借助人工智能的高速运算和自我调整能力，构筑出用户的数据画像。当用户的数据画像被企业所掌握，对个人的隐私以及其他人格权益的影响将超乎一般的处理行为。与此同时，基于数据画像，互联网企业得以有针对性地进行个性化的客户端界面设计、差异化的服务提供以及定向广告推荐。这些额外的数据用途既为用户带来便利与舒适，也可能带来隐私空间的侵扰、价格歧视、广告骚扰等种种后果。此外，自动化决策，或称 AI 辅助决策亦很可能给用户带来有失公平的待遇。[19]基于行为信息的人工智能预判和决策也许在宏观方向上并无谬误，但由于其本质是对用户的内在特征和行为模式的大数据推测，而非确定的事实，故其决策结果一定存在某种偏差。在数据分析技术广泛运用的情形下，对于欠缺专业知识的普通用户而言，用户实际上很难知晓互联网企业对其信息的知晓程度，自然也无从预知互联网企业对其行为信息的上述用途究竟可能带来怎样的后果。[20]故而，倘若企业欲将采集的行为信息用以进行行为化定位等特殊用途，则不仅应在使用目的中进行说明，还应当进行比一般用途更为具体的专门披露。

四、用户同意规范制度的应然设计

（一）用户同意的区别化样式

用户行为信息采集的情境千差万别，所需同意的样式不宜千篇一律，而应有合理的差异性。传统的用户同意规则界分方式，是因由采集或后续处理的情境之

[18] Article 13(2)(f), Article 14(2)(g), Article 15(l)(h), REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[19] 例如，在 “大数据杀熟”案例中技术设计者将能最大化实现其自身利益的代码和算法输入到网络平台程序，在对用户精准画像后，自动分析并预测用户偏好进而形成价格歧视。参见吴梓源、游钟豪：《AI 侵权的理论逻辑与解决路径 ——基于对“技术中立”的廓清》，载《福建师范大学学报(哲学社会科学版)》2018 年第 5 期。

[20] 洪玮铭、姜战军：《社会系统论视域下的个人信息权及其类型化》，载《江西社会科学》2019 年第 8 期。

不同而设置宽严相异的同意规则。这种情境化分析的思路源于自然人隐私保护中将隐私侵害置于特定场景中看待的路径。Nissenbaum 教授提出了个人信息采集、处理和利用中涉及隐私保护的情境完整性理论，[21]基于此，企业对于用户行为信息的采集，理应符合用户对由全部事件、行为、交易等共同构筑的情境下隐私受保护的合理期待。倘若企业的采集行为超出了用户基于情境的合理期待，则将可能有侵害用户隐私之嫌，故而只有在获取用户尤为明确的同意表示后，企业的采集方能具有合法性基础。

在下述两种情境下，企业对用户行为信息的采集应取得用户的明确同意，除此之外的其他情境则一般的同意亦可：一是采集敏感的个人信息。倘使企业所采集的行为信息涉及敏感的个人信息，则在采集时应获取用户的明确同意。二是有特殊的后续处理目的。企业采集用户行为信息既可能是提供网络服务所必须，也可能是为了以个性化方式提高用户体验，还可能是希望借此对用户进行画像，并基于画像之结果进行行为化定位、个性化推荐甚至自动化决策。这些深层次的后续分析将更可能构成对用户人格权益的侵害。故而，倘若用户行为信息在采集后将被用于用户画像或基于此的行为化定位、个性化推荐、自动化决策等目的进行处理，则企业在采集时即应当告知用户并征求其明确同意。[22]

上述传统的用户同意规则界分方式是以采集行为可能对用户带来的后果为导向的。值得注意的是，英国信息专员办公室（Information Commissioner's Office, ICO）于 2012 年将当时互联网企业用于采集用户行为信息的 Cookies 技术群根据采集功能差异划分为四种类型，并规定了所对应的不同的同意样式。这种划分的基础是自动化采集工具所具备的不同功能，因而，倘若某一自动化工具兼具两种以上功能，则应当同时满足各功能对应的同意样式之要求。换言之，无论企业在采集时使用的是 Cookies、Spyware、DPI 还是其他自动化采集工具，都应当按照该工具实际功能所对应的用意样式征求用户之同意。

---

[21] Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 Washington Law Review 119, 136-138 (2004).

[22] Article 22(2)(c), REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

依此区分，可将自动化采集工具区分为下述四类：一是特别必要的工具；二是与服务性能表现有关的工具；三是拥有特定功能的工具；四是用于行为化定位或个性化推荐的工具。其中，特别必要的工具往往是某种 Cookie，其应用仅仅是为用户提供互联网产品或服务之必需，同时所采集的行为信息数量不多。故而，运用此类工具时可允许企业采用择出机制，无须获得用户对于采集的明确同意，而是通过其持续不断的访问行为推定其默示同意，但企业至少应向用户充分披露该采集工具的具体采集行为。至于后三者，则依其在采集用户行为信息的规模、深度和影响上的不同，适用程度不同的征求用户同意之机制——用于行为化定位或个性化推荐的工具在采集功能上表现最为强势，故应适用最为严格的明确同意之样式。[23]与服务性能表现有关的工具和拥有特定功能的工具则介于最宽松与最严格的同意样式之间。

（二）同意形式的改造

欧盟《一般数据保护条例》中用户表示同意的有效形式分成两种，一是表明同意意愿的声明，二是某项清晰的确信行动。[24]前者是主动地述说同意之意愿，乃是传统的同意形式，此处无须赘言。后者是以用户负有确定含义的特定行为昭示用户同意之意愿。笔者认为，这在用户行为信息的自动化采集中具有很强的实践意义。因为在纯粹的网络化环境下，用户通过点击等行为所表示的同意信号能够直接被自动化处理工具所接收，用户行为信息的采集流程将始终得以自动、高效地进行。典型的表示同意的用户行为是于在线的环境下点击复选框。具言之，目前网站或手机 APP 征求用户同意的通行做法是在页面上显示“我同意”“我接受”等类似复选框，用户以双击鼠标左键或手指轻摁的方式点击同意按钮，即可作出同意的意思表示。在高速的互联网时代下，点击的形式尽管便捷有余，可作为用户同意的一般外部表达形式，但显然慎重程度不足，至少不应当成为承载

[23] Robert Bond, *The EU E-Privacy Directive and Consent to Cookies*, 68 Business Lawyer 215, 222-223 (2012).

[24] Article 4(11), REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

用户明确同意的表示形式。

质言之，设置用户明确同意之形式，并不以追求效率为本质，而应将关注点更多地投注于外在表示形式与内在意志内容的一致性和匹配性，促使用户的真实意思能够得到最为准确的表达。比之过于简单、随意的点击方式，电子签名似乎更适宜作为用户明确同意的外在表彰。一是签名行为有缔约的潜在内涵。比起机械性地点击页面或弹窗中的诸多选项，用户在以电子签名形式作出同意时，更能意识到该同意决定与自我之间的联系，以传递用户内心之真意。二是具有多样化的形式，能够兼顾不同的采集情境。我国《电子签名法》并未将电子签名狭义地限定为数字签名，而是以识别签名人与确认签名人认可两项功能为电子签名认定的核心。[25]广义的电子签名认定路径与网络环境下多样的采集情境更为匹配，不同敏感程度的用户行为信息之采集可以采用不同的电子签名形式要求。[26]三是法定的电子签名形式具有经法律确认的效力。电子签名是互联网商业交易普及背景下自然人签字的衍生形式。为便利无纸化电子交易的进行，各国纷纷颁布法案，对电子签名的法律效力加以确认。欧盟于 1999 年制定了《关于建立电子签名共同法律框架的指令》；[27]次年，美国颁布了《全球和国内商业法中的电子签名法案》。[28]我国亦于 2004 年公布《电子签名法》，明确规定可靠的电子签名具有与手写签名同等的法律效力。[29]可靠的电子签名在涉及用户行为信息采集的互联网服务合同场景下能够完全有效地表示用户的缔约意思，这将使得用户的同意拥有确定的合同法律效力，企业依约的采集行为将免于不确定的合规风险。[30]此外，

[25] 参见《中华人民共和国电子签名法》第 2 条。

[26] 广义来看，自动生成的电子签名、输入的签名、识别码、勾选复选框等都属于电子签名形式，只是个人在使用上述不同签名形式时有着由强到弱的感知区别。

[27] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures.

[28] The Electronic Signatures in Global and National Commerce Act (E-Sign Act).

[29] 参见《中华人民共和国电子签名法》（2004 年）第 14 条。该法经历了 2015 年、2019 年两次修正，现行《中华人民共和国电子签名法》（2019 年修订）第 14 条亦作了同样规定。

[30] Patrick Myers, *Protecting Personal Information: Achieving a Balance Between User Privacy and Behavioral Targeting*, 49 Michigan Journal of Law Reform 717, 741 (2016).

对于敏感程度极高的私密信息，一些学者提出要以严于告知同意原则的方式进行采集。[31]于此，可靠的电子签名作为同意形式的效力加强版本，或可成为私密行为信息采集同意的形式要件。

（三）同意的例外——其他采集合法性基础的明确

采集行为的同意，本质上为用户就个人信息进行自决的意思表示，故将用户同意作为企业采集用户行为信息的合法化基础，无疑体现了对私人自治的尊重与保护。然而，尽管私人自治在私法领域中占据着无上的崇高地位，但私人自治不是私法唯一的价值基础。自由从来不能自外于其他人文价值而独存，私法同时还追求正义、平等、安全与效率等其他价值。[32]这些价值追求同样应当经由法律规范而得到明确。《欧盟基本权利宪章》即规定，个人信息处理的正当性基础既可以是用户本人的同意，也可能是基于其他的法定事由。[33]

明确用户同意外的其他采集合法性基础，体现了一种利益冲突与衡量的逻辑进路。首先，行为信息反映了用户的网络化踪迹，是对个体进行数据造像的基础。行为信息的背后当然蕴藏着关乎自然人人格的利益，尤其是自然人的隐私利益。法律规范赋予了自然人对个人信息的自决权能，让用户自己掌控行为信息的去向。这就是将用户同意作为采集行为合法化基础的目的所在。但在用户个体的人格利益之外，用户行为信息采集和运用过程还可能牵涉诸多同样应当得到法律规范保护的利益，这其中既有公共利益，也有其他社会个体的利益。这些利益有着不同的取向，很可能与自然人的人格利益在用户行为信息采集的节点发生冲突。例如，杭州野生动物世界在未征得郭兵同意的情况下，将园区年卡系统升级为人脸识别，郭兵认为园区收集的面部特征等信息属于个人敏感信息范畴，故将杭州野生动物世界告上了法庭。[34]又如，在 2018 年 “晒晒你的支付宝年度账单”活动中，支

[31] 张新宝：《个人信息收集：告知同意原则适用的限制》，载《比较法研究》2019 年第 6 期。

[32] 易军：《私人自治与法律行为》，载《现代法学》2005 年第 3 期。

[33] Article 8 (2), EU Charter of Fundamental Rights.

[34] 朱健勇：《中国人脸识别第一案 杭州一动物园被起诉》，载《北京青年报》2019 年 11 月 4 日，第 A7 版。

付宝以默认勾选的方式隐秘地收集用户信息，随后，中国人民银行杭州中心支行以支付宝实施 7 项违法行为为由，对其开出 18 万元罚单。[35]当认定公共利益或其他社会个体的利益在冲突中应得到优先考量时，即催生出知情同意原则的例外——其他应受法律保护之价值的存在，亦是用户行为信息采集的合法性基础。

这些合法性基础通常包括下述内容：其一，公共利益的需要或政府的强制命令。作为社群主义哲学的产物，公共利益代表了社会中多数人的利益诉求。个人的权利行使并不能够绝对自由，而是要顾及所在社会的公共利益。一旦面临国家安全利益、公共卫生利益或其他重大公共利益受威胁的情形，企业应以公共利益为重，可不经用户同意即采集必要的行为信息。此外，在犯罪侦查等情形下，企业应当遵照政府的强制性命令采集并向其提供相关信息。其二，企业践行法定义务所必要。一些法定义务的承担，需要企业通过采集用户行为信息加以完成。譬如，为维护金融安全，我国从事网络支付业务的互联网企业不仅需要对用户身份采取持续的识别措施，还应当确保用户交易信息的真实、完整与可追溯性。这要求企业对用户的交易类型、金额、时间、对象、大额支付用途和事由等进行记录。其三，为企业或第三方的正当利益之必要。倘若法律设置了此项例外，则企业可以为追求自身或其他用户的合法且正当之利益，在告知用户后径行采集其行为信息。这里的正当利益可能包括支持、维护公司业务经营、网络系统安全、用户信息安全，以及其他重要的商业利益和运营需求。[36]其四，企业履行与用户之间的合同所必要。一些行为信息的采集是出于企业与用户间合同履行所需，如用户欲享受网络购物服务，根据服务协议，企业需采集并储存其浏览记录、购物车信息；在网络社交服务中，社交 APP 需采集用户的点赞、评论等信息用以提供社交互动、参与服务；在快递物流服务中，快递物流平台需采集用户的名址、联系方式、物品名称等信息，以履行安全寄递的服务内容。[37]此时的采集行为以服务合同法

[35] 封寿炎：《支付宝 7 项违法被罚 18 万元，为何说罚少了》，载《解放日报》2018 年 4 月 10 日，第 5 版。

[36] Mike Hintze, *Privacy Statements under the GDPR*, 42 Seattle University Law Review 1129, 1139 (2019).

[37] 参见姚佳：《企业数据的利用准则》，载《清华法学》2019 年第 3 期；孟晓明，贺敏伟：《社交网络大数据商业化开发利用中的个人隐私保护》，载《图书馆论坛》2015 年第 6 期；孟涛：《基于“丰鸟数据之争”的数据财产的法律属性与保护路径》，载《大连理工大学学报（社会科学版）》2019 年第 2 期。

律关系为其合法性基础，无须再取得用户同意。

笔者认为，设置用户同意的例外宜审慎为之。这要求立法者妥善处理知情同意原则与其他合法性基础背后的深层利益冲突，以达到兼顾社会公共利益、商业化的数据需求和用户人格利益的立法目的。应当清楚地意识到，设置用户同意的例外，是对以个人信息私人自治为内在的同意原则之突破。因而，用户同意例外情形之设计应当尽可能地明确，否则，用户同意机制将被诸多的例外所架空，其作为采集合法性基础的效力也将相应地遭到削弱。除此之外，即便是无需取得用户同意的例外情形，企业的告知义务亦不得被豁免。企业应当向用户详细地告知无需取得其同意即可采集的行为信息类别、目的等信息。

The Application and Regulation of the Informed Consent Principle in Information Collection

Zheng Jianing

Abstract: The user's informed consent, as a principle that enterprises should abide by in order to collect users' behavioral information, is the legal basis of users' behavioral information collection. As for the selection and participation mechanism of collection, it is appropriate for China to choose the opt-in regime as the main while structuring the informed consent rules. In its essential premise, the notification process, enterprises should fulfill the obligation to inform users of the following matters, including the genuine subjects of the collection, the categories of behavioral information, the ultimate purpose of use, the afterwards processing behavior and the flow of users' behavioral information to the third party. Special disclosure should also

be utilized for unusual purposes such as behavioral targeting. Designing the users' consent regulation system, the types of users' consent need to be further distinguished, the effective form of consent should be set more prudently, meanwhile, other legal basis of collection apart from the user's consent is clearly defined.

Keywords: data information; information collection; legal basis； informed consent; opt-in regime; opt-out regime