告知同意规则的结构性困境及其纾解：基于美国个人信息立法家长主义探索的启发

沈浩蓝

（西南政法大学 人工智能法学院，重庆 401120）

摘要：由于“有意义的同意”的达致条件难以实现与个人信息共享的不可避免性，告知同意规则面临着结构性困境，其作为个人信息自我管理机制的规范目标无法实现。数据最小化方案是《美国隐私权法案（2024）》对以家长主义克服个人信息自我管理失灵的探索。这一方案对中国纾解告知同意规则的结构性困境具有参考价值，但也存在摒弃同意的道德风险与家长主义立法的僵化风险。中国可构建最小化告知同意方案，一是渐进划定告知同意的最小化范围，对范围外的个人信息处理作出单独同意规定；二是作出实质性透明度要求，包括简化隐私政策以保证告知可读性，细化告知义务以保障用户随时行使撤回同意权。在此过程中，可引入隐私增强技术试点计划，探索平衡个人信息保护与利用的技术之治。

关键词：个人信息；告知同意；《美国隐私权法案（2024）》；家长主义；数据最小化

中图分类号：D923 **文献标志码**：A **文章编号**：2096-028X（2025）01-0066-11

数据是数字经济时代的核心生产要素，个人信息作为数据要素的重要原材料，其处理规则的设计关系到个人信息保护和数据共享利用双重目标的平衡实现。当前，《中华人民共和国民法典》（简称《民法典》）与《中华人民共和国个人信息保护法》（简称《个人信息保护法》）均确立了以告知同意为核心的个人信息处理规则，但被质疑未能发挥应有效用，不仅难以弥合大数据时代显著增大的数据权力差距，[①]也在实践中遭到“流于形式”、未能充分保护公民个人信息权益的质疑。[②] 这些质疑实际上指向了告知同意规则面临的结构性困境。这一困境使得其难以实现个人信息自我管理的规范目标，[③]家长主义的导入成为一种可供讨论的替代方案。[④]

美国于2024年发布的立法提案《美国隐私权法案（2024）》（*American Privacy Rights Act 2024*，简称APRA）搭建了一个以“数据最小化”为基石的个人信息保护框架，反映了美国个人信息立法从自由主义向家长主义的价值转向。2024年4月17日，美国众议院能源与商务委员会创新、数据与商务小组委员会召开了题为“立法保护儿童在线隐私及确保美国人数据隐私权利”的听证会，与会者对APRA的未来通过整体持乐观态度。[⑤] 该法案若获得通过，将在世界范围内创设一种新的个人信息保护范式。尽管在立法传统上，美国对个人信息合规采取“选择退出”机制，告知同意则是一种典型的“选择进入”机制，但二者均为实现个人信息自我管理的途径，是自由主义价值取向的产物，且同样面临着失灵危机。这一共同的价值基础与应用困境，使得APRA对家长主义的探索可以对告知同意规则的结构性困境的纾解有所启示。

基金项目：2024年度重庆市教委科学技术研究计划青年项目“数据知识产权研究”（KJQN202400329），2024年度浙江省哲学社会科学规划青年课题“浙江省数据要素流通交易的法律规则研究”（24NDQN076YB）

作者简介：沈浩蓝，女，法学博士，西南政法大学人工智能法学院讲师。

① 参见王苑：《数据权力视野下个人信息保护的趋向——以个人信息保护与隐私权的分立为中心》，载《北京航空航天大学学报（社会科学版）》2022年第1期，第45-57页。

② 参见丁晓东：《隐私政策的多维解读：告知同意性质的反思与制度重构》，载《现代法学》2023年第1期，第34-48页。

③ Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, Harvard Law Review, Vol.126: 1880, p.1880 (2013).

④ Elettra Bietti, *Consent as a Free Pass: Platform Power and the Limits of the Informational Turn*, Pace Law Review, Vol.40: 310, p.390-392 (2020).

⑤ Lauren Feiner, *A Real Privacy Law? House Lawmakers Are Optimistic This Time*, The Verge (17 April 2024), https://www.theverge.com/2024/4/17/24133323/american-privacy-rights-act-house-lawmakers-legislative-hearing.

一、告知同意规则的结构性困境

告知同意规则在实践中面临的困境并非学者曾经担心的对人格利益的过度保护、妨碍信息流通价值的实现,[①]相反,其受到"流于形式"、未能充分保障用户人格权益的质疑。[②] 这一应用困境的产生可溯源至告知同意规则从医事法领域移植到信息法领域的适应性障碍,实质则为告知同意规则的结构性困境在实证层面的显现。

(一)"有意义的同意"条件难以达致

告知同意原本是医事法领域的一项原则,要求医生对患者进行诊疗活动时,应当向患者详细说明病情、医疗措施、医疗风险、替代医疗方案等相关诊疗事项,并在此基础上取得患者的书面同意,旨在帮助患者践行对自己身体的决定权。该原则发端于 1914 年的美国判例 *Schloendorff v. Society of New York Hospital*,法官在判决中指出:"每一个成年且心智健全的人都有权决定如何处置自己的身体;外科医生如果未经病人同意而实施手术,则构成伤害罪,应承担损害赔偿责任。"该判决确立了患者对自己身体的决定权是告知同意的法理基础。[③] 到 20 世纪 70 年代,德国学者威廉·施泰因米勒(Wilhelm Steinmüller)在撰写个人信息保护法草案时提出信息自决权概念,即认为公民对自己的个人信息拥有如同对自己身体一般的决定权,有权自由决定周遭的世界在何种程度上获知自己的所思所想以及行动。[④] 自此,告知同意被沿用到信息法领域。在 1984 年德国联邦宪法法院的"人口普查案"后,信息自决权在欧洲被发展为一项一般人格权。[⑤] 基于信息自决权这一法理基础,告知同意被认为是对个人自治和人的尊严的尊重和维护,从而成为个人信息收集和利用的正当性基础,并为 1995 年欧盟《数据保护指令》(*Data Protection Directive*)所纳入。[⑥]

将告知同意自动延伸至个人信息领域的做法立足于立法者对"小数据"时代网络技术水平的理解,其适应性障碍随着大数据技术的广泛应用而逐渐凸显。从法律性质上看,个人同意属于违法阻却事由,其功能在于针对那些法益侵害行为发挥正当化的效力。[⑦] 同意体现了法律对个人自主权的尊重。正如杰里米·沃尔德伦(Jeremy Waldron)所言:"因为我们把每一个人看做是潜在的道德主体,天生具有尊严和自治,所以我愿意将自我管理的重担信托给人民全体。"[⑧]基于此,为了实现对假定违法性的反驳功能,个人作出的同意应当是能够体现个人意志的有意义的同意。美国学者尼尔·理查兹(Neil M. Richards)与伍德罗·哈特佐格(Woodrow Hartzog)认为,在理想化状态中,有意义的同意应满足三个"黄金标准",一是对个人同意的请求并不频繁,二是同意可能带来的风险应当生动且易于想象,三是个人能够认真对待每项获取同意的请求。[⑨] 以此检视医事法与信息法领域的告知同意,不难发现,患者作出的同意基本符合"黄金标准"的要求,但互联网用户的同意则不尽然。医方仅在手术治疗需要时向患者作出同意请求,患者可以通过向医方咨询充分了解自己的身体状况、治疗成功率以及手术可能带来的风险或后遗症等。在对获取的信息进行全面研判的基础上,患者作出的同意或拒绝治疗的决定都能较大程度反映其真实意志,是一种有意义的同意。但在个人信息领域,特别是在大数据时代,信息过载导致"有意义的同意"的达致条件难以实现,告知同意规则面临着结构性困境。[⑩]

大数据的体量决定了个人信息处理者不可能向每一名用户就被收集的个人信息的利用方式和去向进行充分解释和磋商。为了规避侵权风险与提高效益,个人信息处理者普遍通过设置用户隐私政策以获取同意

---

① 参见高富平:《论个人信息保护的目的——以个人信息保护法益区分为核心》,载《法商研究》2019 年第 1 期,第 93-104 页。

② 参见丁晓东:《隐私政策的多维解读:告知同意性质的反思与制度重构》,载《现代法学》2023 年第 1 期,第 34-48 页。

③ *Schloendorff v. Society of New York Hospital*,211 N.Y. 125,105 N.E. 92(N.Y. 1914).

④ 参见杨芳:《个人信息自决权理论及其检讨——兼论个人信息保护法之保护客体》,载《比较法研究》2015 年第 6 期,第 23 页。

⑤ 参见杨芳:《个人信息自决权理论及其检讨——兼论个人信息保护法之保护客体》,载《比较法研究》2015 年第 6 期,第 23 页。

⑥ *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*,European Union (23 November 1995),https://eur-lex.europa.eu/eli/dir/1995/46/oj/eng.

⑦ 参见程啸:《论个人信息处理中的个人同意》,载《环球法律评论》2021 年第 6 期,第 47 页。

⑧ [美]杰里米·沃尔德伦:《法律与分歧》,王柱国译,法律出版社 2009 年版,第 293 页。

⑨ Neil M. Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, Washington University Law Review, Vol. 96: 1461, p. 1492-1498 (2019).

⑩ 参见吕炳斌:《个人信息保护的"同意"困境及其出路》,载《法商研究》2021 年第 2 期,第 89-90 页。

的方式满足个人信息处理的合规要求。然而,隐私政策无法起到令用户“被充分告知”并基于此作出符合自身意愿的“同意”的作用,其内容往往非常冗长而复杂,需要耗费用户大量时间和精力方能阅读并理解全部内容。2022年美国的一项隐私政策研究表明,就全球范围内高访问量网站所采用的隐私政策文本而言,其篇幅已达1996年的4倍,平均每份文本增加超过4 000个单词,可读性却趋于下降。① 高度数字化的当代社会生活充斥着来自个人信息处理者的隐私政策,信息过载带来的同意疲劳令告知同意规则对个人信息处理风险的警示作用被严重削弱。②

(二)个人信息共享具有不可避免性

个人信息共享的不可避免性进一步加剧了告知同意规则的结构性困境。在告知同意规则中,“告知”是“同意”的前提,个人信息处理者应充分履行告知义务,个人基于对个人信息处理情况的知悉与研判所作出的“同意”才是能够体现其意志的、有效的同意,方能成为个人信息处理的正当性基础。但在互联网环境中,用户对作为个人信息处理者的网络服务提供者的个人信息共享通常具有不可避免性,表现为个人有时无法阻止个人信息的共享或同意并非总是基于充分知情与自愿而作出。③ 造成这一现象的原因较为复杂,主要包括以下方面:第一,互联网作为一项受到普遍认可的基础性服务,在生活便利、教育普及、公共医疗、工作社交等方面发挥着重要作用。用户为了确保自身能够获取并充分利用这些服务,向网络服务提供者共享个人信息已成为必要条件。第二,网络服务提供者,特别是大型互联网平台,凭借在发展初期积累的大量数据资源,建立起显著的市场优势,甚至具有市场支配地位。在这种情况下,个人拥有的交易选择非常有限,甚至不存在可行的替代选项。第三,相较于投入时间、金钱资源寻找与获取替代交易方案,大多数普通用户会接受网络服务提供者的个人信息共享要求以规避转换成本。第四,大量网络服务提供者提供的用户隐私政策存在透明度不足的问题,将影响用户对个人信息处理情况的充分认知。④

不仅如此,这些隐私政策本质上是一种格式条款,用户无法对其内容提出任何异议或修改请求,如果不允许网络服务提供者收集和利用其个人信息,就无法使用其提供的服务和产品。这种“全无/全有”的模式事实上制约了用户信息自决权的践行,用户“除了同意外几乎别无选择”。⑤ 因此,用户虽然在理论上拥有不同意个人信息被获取的权利,但由于网络服务的基础性、用户与个人信息处理者关系的不对等、替代交易方案的获取成本等原因,为了免于遭受严重的不便利甚至利益损害,用户对个人信息的共享实际上不可避免。此时,用户同意与个人意愿无关,即使个人信息处理者提供了十分详尽的用户隐私政策,对于用户而言,既然对同意的作出不可避免,不加阅读直接同意隐私政策更加符合效率原则,详细阅读具体条款除了徒增时间、精力上的浪费之外,对用户本人并无实质意义。美国一项实证研究显示,74%的实验对象在获取社交网络服务时,直接跳过了对隐私政策的阅读;在未选择快速跳过隐私政策的实验对象中,对隐私政策的平均实际阅读时间仅为73秒,但该文本正常阅读所需时长约为30分钟左右。但尽管该隐私政策基本未被实际阅读,高达97%的实验对象均选择同意该隐私政策。⑥ 这一研究结果直观地表明,告知同意不过是一纸空文,所谓的用户同意客观上沦为用户对不可避免的个人信息共享的妥协。这一困境实为大数据时代个人信息共享的不可避免性与通过告知同意实现信息自决的立法追求之间的矛盾。

二、美国个人信息立法的家长主义转向

告知同意的结构性困境意味着其作为个人信息自我管理实现规范的落空,家长主义的导入成为一种可供讨论的替代方案。APRA对“数据最小化”方案的创设反映了美国个人信息立法的家长主义价值转向。告

---

① Chris Stokel-Walker, *Privacy Policies Are Four Times as Long as They Were 25 Years Ago*, New Scientist (3 February 2022), https://www.newscientist.com/article/2307117-privacy-policies-are-four-times-as-long-as-they-were-25-years-ago.

② Rishab Bailey & Smriti Parsheera, et al., *Disclosures in Privacy Policies: Does "Notice and Consent" Work?*, Loyola Consumer Law Review, Vol. 33:1, p.2 (2022).

③ Laura M. Moy, *Unavoidability in U.S. Privacy Law*, Columbia Science and Technology Law Review, Vol.25:56, p.58 (2024).

④ Laura M. Moy, *Unavoidability in U.S. Privacy Law*, Columbia Science and Technology Law Review, Vol.25:56, p.59-65 (2024).

⑤ 参见任龙龙:《论同意不是个人信息处理的正当性基础》,载《政治与法律》2016年第1期,第128-131页。

⑥ Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, Information, Communication & Society, Vol.23:128, p.128 (2020).

知同意规则与美国过往采取的选择退出机制均为实现个人信息自我管理的途径,是自由主义价值取向的产物,且同样面临着失灵危机。这一共同的价值基础与应用困境,使得 APRA 对家长主义的探索可以对告知同意规则的结构性困境的纾解有所启示。

(一)立法价值的转向契机

近年来,面对国内外对美国个人信息隐私保护力度不足的批评,美国致力于建立联邦层面统一的个人信息保护立法,这成为个人信息立法家长主义价值转向的契机。

长期以来,美国在信息隐私领域的立法以促进信息数据自由流通和便捷交易为要。个人信息被认为具有工具性价值,将其投入生产领域有助于增加财富和社会效用,以保护之名限制信息流动不利于社会财富最大化。① 这一认知契合了美国在第二次世界大战后的技术政策指导理念,即以技术发展作为国家进步与生存之要。② 基于这一指导理念与立法偏好,美国传统上对个人信息的保护呈现以下特点:第一,美国并未如欧盟一般为公民创设作为基本权利的个人数据权,而是将个人信息作为消费者隐私权益予以保护,力图在隐私与有效的商业交易之间取得平衡。③ 第二,美国采用选择退出机制,允许通过推定同意实现个人信息处理合规。个人信息处理者在向用户发布以同意为默认选项的隐私政策后,若用户继续使用其提供的服务或未明确予以拒绝,则推定其同意对个人信息的处理。与之相反,告知同意规则要求个人信息处理者获取用户的明示同意,是一种典型的选择进入模式。第三,美国过往并没有联邦层面的隐私权法,隐私权保护框架由针对不同行业、特定类型数据、特定数据主体的法规共同拼凑而成。这种分散式保护模式创造了个人信息保护的动态环境,据此,美国不同州、不同行业之间可能遵循不同的个人信息保护标准。

美国民众对个人信息的收集与处理的怀疑肇始于 2013 年美国国家安全局前情报承包商爱德华·斯诺登(Edward Snowden)对“棱镜计划”的曝光。④ 此后,隐私丑闻的频繁发生与欧盟在个人信息保护领域的积极作为引发了美国公众对个人信息保护不足的忧虑。美国无党派智库皮尤研究中心(Pew Research Center)在 2019 年进行的一项针对 4 272 名美国成年人的隐私态度抽样调查显示,72%的受访者认为自己的线上活动受到科技公司与广告商的普遍追踪,80%左右的受访者则认为自己对被收集的个人信息缺乏控制力、对个人信息处理方式缺乏了解、个人信息被收集的潜在风险大于获益等,表达了对信息隐私安全的忧虑。⑤ 拼凑式立法被认为在数据隐私世界创造了一种“狂野西部”环境,引发了美国立法者对其互联网隐私监管格局的重新审视。⑥

在这一背景下,加利福尼亚州于 2018 年首开先河,颁布了美国国内最为严格的个人信息保护法案《2018 年加利福尼亚州消费者隐私保护法案》(*California Consumer Privacy Act of 2018*),标志着美国个人信息与隐私立法新时期的到来。此后,弗吉尼亚州、科罗拉多州等相继颁布了本州的隐私法案。上述法案摒弃了对个人信息的分散式保护传统,普遍适用于一切符合条件的处理本州居民个人信息的个人信息处理者,并提高了消费者个人信息保护标准。在各州全面隐私立法实践的基础上,美国国内对建立联邦层面的统一的网络隐私法的呼声也日益高涨。2022 年 7 月,美国众议院能源和商业委员会通过了民主党与共和党合作制定的《美国数据隐私和保护法案》(*American Data Privacy and Protection Act*,简称 ADPPA),旨在实现对个人信息处理者保存和使用消费者个人信息行为的监管。由于隐私执法力度不足、与各州隐私法案关系不明确以及规定措施存在争议等,ADPPA 遭到了多方反对,立法议程被冻结,但美国国内对制定个人信息保护的联邦标

---

① Richard A. Posner, *The Right of Privacy*, Georgia Law Review, Vol.12:393, p.394-409(1977).

② David M. Hart, *Forged Consensus: Science, Technology, and Economic Policy in the United States, 1921—1953*, Princeton University Press, 1998, p.3-29.

③ Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, California Law Review, Vol. 102:877, p.887(2014).

④ Emily Stackhouse Taetzsch, *Privacy Purgatory: Why the United States Needs a Comprehensive Federal Data Privacy Law*, Journal of Legislation, Vol.50:121, p.144(2021).

⑤ Brooke Auxier & Lee Rainie, et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information*, Pew Research Center(15 November 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information.

⑥ Emily Stackhouse Taetzsch, *Privacy Purgatory: Why the United States Needs a Comprehensive Federal Data Privacy Law*, Journal of Legislation, Vol.50:121, p.122(2021).

准的呼声并未减弱。2023年2月,美国时任总统拜登在发表的国情咨文演讲中,呼吁对大型科技公司个人信息收集行为进行更严格的限制,这表明个人信息保护的紧迫性已成为美国的主流认知。[①] 2024年4月7日,美国众议院能源和商业委员会主席凯茜·麦克莫里斯·罗杰斯(Cathy McMorris Rodgers)与参议院商业、科学和运输委员会主席玛丽亚·坎特韦尔(Maria Cantwell)共同发布APRA。APRA作为ADPPA的后继法案被推出,以建立美国统一的消费者数据隐私权为中心,搭建了一个以数据最小化为基石的个人信息保护框架,承载着两党在隐私监管领域的共同愿景。

(二)APRA的核心内容

从立法追求来看,美国立法者对APRA寄予的期待主要包括三点:一是通过APRA这项联邦层面的立法解决美国长期以来个人信息保护立法的"拼凑"问题;二是实现个人信息保护与信息数据流通利用之间的平衡;三是避免美国的个人信息立法重蹈欧盟告知同意的覆辙,成为一个空洞的法律结构。为实现以上目标,APRA搭建了一个以数据最小化为基石的个人信息保护框架。

1.数据最小化原则

APRA要求个人信息处理者对用户个人信息的收集、处理、保留或转移(统称处理)应当遵循数据最小化原则。据此,个人信息处理者仅被允许为以下目的,在必要、适度而有限的范围内处理个人信息,分别是:提供或维护个人请求的特定产品或服务;在与用户关系范围内进行符合个人合理预期的通信;APRA明确规定的法定事由。其中,APRA列举的法定事由可按照处理目的的不同被分为三类。

一是基于服务提供需要处理用户个人信息,包括:提供或维护用户请求的特定产品或服务;产品召回或保修;开展市场调研;为改进产品、服务或开展科学研究等将数据去识别化;通信服务商提供呼叫位置信息;为用户提供第一方或上下文广告;为用户提供指导类与新闻类定向广告。

二是基于自身经营原因处理用户个人信息,包括:为自身进行法律索赔;企业重组时将用户个人信息转移给第三方,但需要告知该用户并提供第三方的相关信息,用户有权要求撤销此前的同意并删除个人信息。

三是基于法定或公共义务处理用户个人信息,包括:保护数据安全与网络安全;为遵守其他法定义务;根据合法程序向执法机构传输数据;为预防或应对欺诈或骚扰行为;为预防或应对具有紧迫性的现实或网络安全事件;为预防或应对具有紧迫性的公共安全事件;为预防或应对犯罪活动。

对于敏感个人信息的处理应当基于APRA明确列举的上述法定事由。个人信息处理者向第三方转移敏感个人信息的,应当向用户发送清晰醒目、通俗易懂的转移申请,获得用户的明示同意,并提供与同意选项同样清晰醒目的拒绝同意选项和撤回同意方式。对于其中的生物识别信息与遗传信息,APRA进一步限制了允许处理的目的范围,要求个人信息处理者就此类信息的所有处理行为获得用户的明示同意,并遵循对此类信息的法定留存期限。该期限为用户明确同意的期限或个人信息处理者与用户最后一次互动起3年,以其中更靠前的期限为准。

2.隐私政策透明度要求

个人信息处理者对隐私政策的公开应满足透明度要求,包括形式与内容两方面。形式要求表现为个人信息处理者应当以清晰醒目、准确易读且易于获取的方式公开隐私政策,说明其个人信息处理活动;提供隐私政策的多种翻译版本与无障碍版本;当隐私政策发生重大变更时,以清晰醒目的方式提前通知用户并提供退出选项。内容要求是指该隐私政策应当包括但不限于以下实质内容:个人信息处理者的身份信息与联系方式;处理的数据类别与处理目的;数据传输的第三方信息与传输目的;数据保留期限;用户对其个人信息行使权利的显著说明;数据安全说明;隐私政策生效日期;数据跨境情况说明等。

APRA对大型数据持有者规定了更严格的透明度标准。大型数据持有者不仅需要遵循上述要求,且应当保留并公布隐私政策的各个历史版本10年以上,并向用户发送清晰醒目、准确易得的500字以内的通知,说明数据处理情况与用户权利内容。联邦贸易委员会(Federal Trade Commission,简称FTC)应当发布此类通知的指导模板。

---

① Joe Garofoli, *Biden Seizes on the Rare Bipartisan Rallying Cry: Regulate Silicon Valley, President Called for Stronger Transparency Requirements on Tech Companies*, San Francisco Chronicle (8 February 2023), https://www.sfchronicle.com/politics/article/biden-sotu-tech-17769680.php.

3.用户的个人信息权利

用户对个人信息享有控制权与选择退出权。控制权是指用户对其个人信息享有访问、更正、删除、导出等权利,个人信息处理者应对用户的该权利行使予以配合。在收到用户请求后,个人信息处理者原则上应当在 30 日(大型数据持有者为 15 日)内以可读取的格式向用户提供其个人信息、更正不准确或不完整的信息、删除或导出用户个人信息。用户一年内可以免费行使 3 次以上权利,超出该次数限制的,个人信息处理者可以收取合理费用。

选择退出权对个人信息处理者作出了三个要求:一是提供清晰醒目的拒绝或退出机制,保证用户选择不接受数据传输的权利和退出定向广告的权利。二是引入用户集中同意与退出机制,通过设置具有用户友好、无障碍性、无冲突性等特征的“选择退出偏好信号”以便用户能够通过单一界面行使选择退出权。三是对“后果性决策”的告知义务。个人信息处理者使用算法分析用户数据、协助用户作出决策的,此类算法决策如果将影响用户对住房、就业、教育机会、医疗保健、保险或信贷机会等重大利益事项的获得或平等享有,或者影响用户对公共场所的自由进出,应当通知用户并让其选择是否使用该算法,同时尊重个人选择退出使用的权利。

4.个人信息处理者的义务

个人信息处理者除了应保障用户权利的实现外,还需要遵循以下义务。一是禁止干涉用户权利的义务。个人信息处理者不得采用“暗黑模式”①分散用户对通知的注意力,妨碍用户对其权利的行使,直接获取、推断或引导用户作出同意;也不得对用户权利的行使条件进行虚假或重大误导性陈述,从而妨碍或限制用户自主权的行使。二是禁止拒绝服务的义务。个人信息处理者不得因为用户对其个人信息权利的行使而通过服务或定价对用户进行报复,包括不得拒绝提供服务,不得对产品或服务收取不同的价格或费率,不得提供不同质量水平的产品或服务。三是数据安全保护义务。个人信息处理者应当建立数据安全实践,以确保用户个人信息的保密性、完整性和可访问性,并免受未经授权的访问。为此,个人信息处理者应至少完成对数据处理系统的定期风险评估、风险预防与纠正、永久性销毁法律要求删除的数据、对员工进行数据保护培训、建立数据安全事故响应程序、指定隐私官和数据安全官等操作。

5.隐私增强技术试点计划

APRA 要求 FTC 实施为期 3 年的隐私增强技术试点计划,鼓励有能力使用隐私增强技术的个人信息处理者自愿申请加入该计划。隐私增强技术这一概念尚未有统一定义,APRA 将其界定为在不危及信息隐私和安全的情况下提取信息价值的任何软件或硬件解决方案、加密算法或其他技术,列举了同态加密、差分隐私、零知识证明、合成数据生成、联合学习、安全多方计算等技术。加入该试点计划的个人信息处理者应当使用隐私增强技术进行符合或超过 APRA 要求的数据安全实践,FTC 将对参与者的实践情况进行审查,确保其将该技术应用于个人信息处理活动中。FTC 发现参与试点计划的个人信息处理者未按照承诺使用该技术的,应通知该参与者,确定其是否继续使用该技术。参与者可在接到通知后的 180 天内予以改正,在规定期限内未予改正的,FTC 将取消其参加试点计划的资格。APRA 要求 FTC 持续发展更多公共部门与私营部门参与隐私增强技术试点计划,并在试点计划期满后形成项目报告。该报告将成为该技术后续推行的重要参考。

三、美国数据最小化方案合理性分析

尽管 APRA 的产生旨在回应公众对个人信息保护不足的忧虑,且不乏受到欧盟《一般数据保护条例》(*General Data Protection Regulation*,简称 GDPR)高水平个人信息保护标准的外部激励,但美国立法者并未考虑引入告知同意规则。这一方面是基于美国对个人信息共享不可避免性的深植观念,即无论如何强化用户同意的地位与价值,都无法改变告知同意沦为一个“空洞的法律结构”的事实。② 更为重要的是,告知同意与

① 即用户界面的设计或操作能够导致诱导或操纵用户行为的实质性后果。

② Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, Boston University Law Review, Vol.104:593, p.604 (2024).

选择退出的本质均为个人信息自我管理机制,二者的核心区别仅在于对“同意”的定义不同,前者仅限于明示同意,后者允许推定同意。在高度数字化的当代社会,信息过载带来的同意疲劳令“有意义的同意”的获取条件难以达致,二者面临着同样的失灵困境。实际上,告知同意对个人信息带来的潜在风险可能高于选择退出,后者的模糊性使得个人信息处理者将较为审慎,明示同意反而更可能异化为个人信息处理者侵权的挡箭牌。①

个人信息立法的家长主义探索致力于回答这一问题:如果同意无法实现用户对自己信息的决定与控制,如何保障用户的隐私权不受损害?对此,美国立法给出的方案是,以数据最小化作为个人信息处理的合法性基础,通过对这一概念的实在化,辅之以对透明度要求的强化、个人信息处理者义务的赋予与技术之治的引入,反向保障用户的个人信息不受滥用。

一是对“数据最小化”概念的实在化。数据最小化并非由 APRA 所首创,这一概念“贯穿于与个人信息相关法律的历史”,被认为是“个人信息保护的基石性原则”,在多国个人信息保护立法中均有所涉及。② 但与此前的立法文件的原则性、宣誓性规定不同,APRA 对数据最小化概念予以实在化,通过明确规定允许个人信息处理的范围以清晰划定其外延边界,赋予这一概念以实操价值。据此,个人信息处理者对用户个人信息的收集和使用被限制在用户与之互动过程中所期望的处理范围内,不得超出提供或维护特定产品或服务所必需的适度而有限的范围。此举改变了美国在信息隐私领域的自由主义立法传统,美国对个人信息处理活动的规范立场从“以允许为原则”转变为“以禁止为原则”,将从源头上限制广泛且非必要的个人信息收集行为。

二是对用户个人信息的反向保障。APRA 整体呈现“重告知无同意”的特点。“无同意”意味着在数据最小化模式下,个人信息处理不以用户同意为合法性基础,对用户个人信息权利的保障有赖于对个人信息处理行为的规范。APRA 要求个人信息处理者保障用户对个人信息的控制权与选择退出权,又通过规范其服务提供行为以确保用户个人信息权利行使不受妨碍,从而保证数据最小化不受滥用。为此,APRA 非常重视对用户充分知悉个人信息处理情况的保障,对个人信息处理者作出了严格的隐私政策透明度要求,以便用户随时行使选择退出权与撤回同意权,拒绝非必要的信息共享。

三是对敏感个人信息的区分保护。APRA 要求个人信息处理者对敏感个人信息的处理应当基于明确列举的法定事由。对于将敏感个人信息向第三方转移、处理生物识别信息与遗传信息的情形,APRA 允许的目的范围更为狭窄,且要求获得用户的明示同意。这些规定体现出 APRA 基于信息敏感程度的个人信息分级保护思路,即个人信息的敏感度越强,处理行为受到的限制就越大。这一区分思路也与用户有效同意的获取难度相匹配。个人信息处理者仅在以上情形发生时向用户请求同意,同意请求不频繁,向第三方转移敏感个人信息、处理生物识别信息与遗传信息的风险生动且易于想象,因此用户将会更为审慎认真地对待此类请求,更有可能作出有意义的同意。

四是对技术之治的探索。技术治理有助于矫正法律的滞后性,并克服法律的模糊性。③ APRA 引入隐私增强技术试点计划,为数据最小化方案的落地提供技术支撑。隐私增强技术是新兴的数据安全监管工具,能够同时满足高效利用数据资源与显著降低对个体数据的采集与加工需求,有望在技术层面实现个人信息保护与数据共享利用的平衡。

整体而言,数据最小化方案是美国对以家长主义克服个人信息自我管理失灵的探索,这一思路能够为中国带来启示。告知同意规则面临着难以克服的结构性困境,无论立法如何强调与强化用户同意,都无法实现其最初预设的通过同意保障公民信息自决的功能。数据最小化方案作为一种家长主义的管制能够辅助个人信息自治的实现。这一思路对中国具有参考价值与可行空间。从个人信息保护的价值取向和功能定位来看,中国并未如欧盟一般将个人信息上升到基本权益的高度,而是将其作为公民人格权益加以保护。相较于 GDPR 将告知同意作为公民信息自决权实现的途径,中国立法倾向于将其作为个人信息处理者的合规手段,

① 参见万方:《隐私政策中的告知同意原则及其异化》,载《法律科学》2019 年第 2 期,第 1-8 页。
② 参见朱悦:《技术与市场之间——试论个人信息最小化原则的理解和适用》,载《经贸法律评论》2021 年第 6 期,第 16-25 页。
③ 参见王燃:《论网络暴力的平台技术治理》,载《法律科学》2024 年第 2 期,第 125 页。

以规范处理行为反向保护用户人格权益,实现个人信息保护与利用的平衡。① 这从《个人信息保护法》的立法目的即可窥见。《个人信息保护法》第 1 条即规定了该法以“保护个人信息权益,规范个人信息处理活动,促进个人信息合理利用”为目的。其中,“保护个人信息权益”和“促进个人信息合理利用”分别指向个人信息所承载的人格利益与经济利益,二者之间存在着一定的张力。这种张力实际上是个人信息的个人性与公共性冲突在实证中的对峙所致。② “规范个人信息处理活动”兼具手段性与目的性价值,立法试图通过利益平衡导向的处理规则实现个人信息保护与利用之间的协调。因此,提倡与探索个人信息立法的家长主义价值转向在中国不会面临太大阻力。

四、中国最小化告知同意方案的设想

应当认识到,告知同意规则虽面临着结构性的困境,却取得了叙事上的成功。在叙事学视野下,告知同意是一套成功的叙事。③ 在域外,从施泰因米勒对信息自决权的提出到德国“人口普查案”的发展,再到欧盟《数据保护指令》对“个人数据权”的确立,这些关键历史素材的选择性挖掘塑造了告知同意从医事法到信息法的基础性地位的延伸;在域内,《全国人民代表大会常务委员会关于加强网络信息保护的决定》对告知同意的引入、“徐玉玉电信诈骗案”和“清华大学某教授电信诈骗案”的发生、《民法典》和《个人信息保护法》对以告知同意为核心的个人信息处理规则的确立,都令告知同意获得了广泛的听取与认同。同意作为个人自治的手段,体现了法律对个人自主权的尊重,具有强大而持久的道德基础。④ 对同意的摒弃易于引起公众的道德反弹,取缔告知同意的做法在中国不具备现实基础。⑤ 因此,中国可在保留告知同意的前提下,参考 APRA 的数据最小化方案,将告知同意的适用限制在法定最小化范围里,并作出相应的立法调适,从而实现对尊重告知同意叙事价值与导入家长主义克服自治失灵二者的平衡。

(一)最小化范围的渐进划定

鉴于理性不及的必然性,立法者对最小化法定事由的预判并不总是与社会现实需要相契合,可能导致数据共享效率的低下并产生额外的成本。目前有学者质疑 APRA 列举的个人信息处理事由“既不反映现有数据生态系统中的商业现实,也不符合消费者的合理期望”,且多停留在市场研究、产品开发、合并与收购等商业层面,未顾及非营利组织的个人信息处理目的,可能进一步导致抑制言论自由的风险。⑥ 查尔斯·林德布洛姆(Charles Lindblom)认为,由于完全理性的不可能,对最佳决策的追求是得不偿失且无法达到的,“切实可行的政策只是与现行政策逐渐地或稍为不同的政策”,决策者应“专注于政策的逐步或微小改变”,确保对现有方案所作出的最终调整仍在其可控范围之内。⑦

对于告知同意最小化范围的划定应基于渐进主义思路。个人信息处理者能够基于同意处理用户个人信息的范围应当被限制在用户与之互动过程中所期望的处理,不得超出提供或维护特定产品或服务所必需的适度而有限的范围。对于具体允许目的的规定,可采用“列举+概括式”立法模式,并区分对待作为个人信息处理者的私营部门和公共部门。其中,对私营部门的允许事项的规定可参考 APRA 所列事项,结合中国行业实践进行相应调整;对公共部门的允许事项的确定可参考各部门对主要个人信息处理事项的类型化梳理。兜底条款可规定为“法律、行政法规规定的其他情形”,为今后在实践中形成共识的个人信息处理新事项的纳入提供开放空间。对于列举事项之外的个人信息处理活动是否属于为提供特定产品或服务所必需以及是

---

① 这一差异着重体现于 GDPR 与《个人信息保护法》规定的用户同意认定标准的差距。GDPR 要求有效的同意应当针对具体的、细化的事项,而中国仅对特定个人信息处理事项规定了用户单独同意要求。

② 参见齐爱民、李仪:《论利益平衡视野下的个人信息权制度——在人格利益与信息自由之间》,载《法学评论》2011 年第 3 期,第 37-44 页。

③ 参见陈一峰:《叙事、叙述与话语权:一个国际法的叙事学研究》,载《云南社会科学》2024 年第 3 期,第 40-49 页。

④ Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, Boston University Law Review, Vol.104:593, p.628 (2024).

⑤ 鉴于中国个人信息立法并不允许以沉默为同意的方式,在中国语境下,同意特指基于告知的明示同意。

⑥ Lothar Determann, Brian Hengesbaugh & Avi Toltzis, *American Privacy Rights Act: A First Glance at the US Congress's Newest Comprehensive Privacy Bill*, Journal of Data Protection & Privacy, Vol.6:375, p.386(2024).

⑦ 参见[美]查尔斯·林德布洛姆:《决策过程》,竺乾威、胡君芳译,上海译文出版社 1988 年版,第 37-42 页。

否符合用户与之关系中的合理预期,应采取个案认定标准,由法官在司法实践中认定。

此外,APRA对涉及敏感个人信息的处理作出了更为严格的规定。中国对敏感个人信息及其他几项对用户有重大影响的个人信息处理行为作出了获取单独同意的规定,相关规定对用户利益的保障更为到位,也具有获取有意义的同意的较大现实性,应对此予以保留。为避免最小化告知同意在实际应用中的僵化,也尊重用户对个人信息的自治要求,对于最小化范围之外的个人信息处理可参照上述规定,即要求个人信息处理者对该事项进行专门告知并获取用户的单独同意。

(二)对透明度的实质性要求

ARPA呈现"重告知无同意"的特点,不以同意为个人信息处理的合法性基础,但强化透明度要求以保障用户知晓个人信息处理情况,随时行使选择退出权。但在最小化告知同意下,由于同意仍被保留,对隐私政策透明度的进一步强化无法改变用户在同意前通常不会认真阅读隐私政策的现状,告知同意的结构性困境仍无法改变。因此,中国应对个人信息处理者作出实质性透明度要求,表现为"简化"与"细化"两方面。

"简化"是指立法对个人信息处理者课以简化告知内容、保证告知可读性的义务。在域外的行业实践中,存在"隐私偏好平台"(platform for privacy preferences,简称P3P)与"隐私营养标签"(privacy nutrition label)两种机制。[①] P3P机制要求网络服务提供者在其服务器的指定位置放置P3P文件,使得详细的隐私政策能够被翻译为以P3P格式编写的压缩版政策,并与用户在网站设置的隐私偏好相比较,自动得出该网站是否符合用户隐私偏好的结论。隐私营养标签机制则是将个人信息处理中的关键问题提取出来加以格式化,方便用户快速浏览与直观感受该网站的隐私保护力度。这两种机制都通过对隐私政策的简化确保告知的可读性,从而提高对"有意义的同意"的获取几率,保证用户的自主权。在现阶段,可通过行业实践探索隐私政策简化机制,并通过司法中对个人信息处理者告知义务的认定引导行业实践,待实践成熟时将其相关做法上升为国家法律。

"细化"是指在引入简化机制的基础上,进一步细化个人信息处理者的告知义务。与APRA用较大篇幅规定了详细的用户自主权保障措施相较,中国立法相关规定较为粗放。中国可参考APRA的透明度要求,规定个人信息处理者需提供隐私政策的多种翻译版本与无障碍版本;在隐私政策发生重大变更时,个人信息处理者需向用户发送清晰简短的通知,说明隐私政策变更情况、法律根据以及变更后对用户的可能影响,相关部门或行业协会应提供通知模板;对于对用户有重大影响的个人信息处理行为,无论是否涉及敏感个人信息,均应当获得用户的单独同意;对于采取"暗黑模式"诱导用户同意的个人信息处理者予以行政处罚等。细化告知义务的目的是保障用户对撤回同意权的随时行使,为此,个人信息处理者还应对网络界面采取"撤回同意友好型"设计,确保用户能在同一界面中完成接受同意、拒绝同意与撤回同意的任何操作。

(三)探索隐私增强技术试点计划

APRA引入隐私增强技术试点计划,探索平衡个人信息保护与利用的技术之治,为中国提供了一定的启示。现阶段,隐私增强技术种类繁多,且处于不断革新、扩容的状态。经济合作与发展组织在2023年发布的《新兴的隐私增强技术:当前的监管和政策方法》报告中,将常见的14种隐私增强技术根据应用方向分为数据混淆、加密数据处理、联合和分布式分析以及数据问责四大类,并详细分析了各项技术的优势与缺憾(详见表1,内容来源于该报告)。[②]

整体而言,隐私增强技术具有广阔的应用前景,但仍存在技术不完全可靠导致隐私泄露、技术应用成本较为高昂、各类技术成熟度不尽相同等局限性。因此,中国在现阶段不宜将采取隐私增强技术作为个人信息处理者的法定义务,可参考APRA引入隐私增强技术试点计划,由相关主管部门牵头,制定详细的试点计划,明确时间表、任务分工与风险管理等;全面调研、对比分析各类隐私增强技术,选取系统稳定、先进且易于部署推广的技术方案;制定标准规范,建立合规评估机制。在此基础上,利用多种渠道宣传隐私增强技术的

---

① Lorrie Faith Cranor, *Necessary but not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, Journal on Telecommunications & High Technology Law, Vol.10:273, p.279-294(2012).

② OECD, *Emerging Privacy Enhancing Technologies: Current Regulatory and Policy Approaches*, OECD(8 March 2023), https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/03/emerging-privacy-enhancing-technologies_a6bdf3cb/bf121be4-en.pdf.

价值,通过政策优惠、技术支持等方法鼓励企业自愿申请加入该计划。

表 1　主要隐私增强技术

类型	关键技术	主要应用方向
数据混淆	匿名化/假名化	安全存储
	合成数据	隐私保护机器学习
	差分隐私	扩大研究机会
	零知识证明	无需披露即可验证信息(例如年龄验证)
加密数据处理	同态加密	1.计算同一组织内的加密数据 2.计算过于敏感而不能公开的私人数据 3.联系人追踪/发现
	多方计算(含隐私集合求交)	
	可信执行环境	使用需要保密的模型进行计算
联合和分布式分析	联邦学习	隐私保护机器学习
	分布式分析	
数据问责	问责系统	1.制定并执行有关何时可以访问数据的规则 2.对数据控制者的数据访问进行不可更改的跟踪
	阈值秘密共享	
	个人数据存储/个人信息管理系统	为数据主体提供对自己数据的控制

五、结语

个人信息立法的家长主义探索致力于回答这一问题:如果同意无法实现用户对自己信息的决定与控制,如何保障用户的隐私权不受损害?对此,美国立法给出的方案是,以数据最小化作为个人信息处理的合法性基础,通过对这一概念的实在化,辅之以对透明度要求的强化、个人信息处理者义务的赋予与技术之治的引入,保障用户个人信息不受滥用。这一思路对中国纾解告知同意规则的结构性困境具有参考价值,但也存在摒弃同意的道德风险与家长主义立法的僵化风险。中国可在保留告知同意的前提下,将告知同意的适用限制在法定最小化范围里,并作出相应的立法调适,从而实现对尊重告知同意叙事价值与导入家长主义克服自治失灵二者的平衡。

Structural Dilemma and Its Alleviation of the Informed Consent Rules: Inspired by the Exploration of American Paternalism in Personal Information Legislation

SHEN Haolan

(School of Artificial Intelligence and Law, Southwest University of Political Science and Law, Chongqing 401120, China)

Abstract: China's personal information processing rules are centered on the informed consent framework, where users must agree to the collection and use of their data. However, significant structural challenges have made these rules less effective in protecting personal data. One major challenge lies in the vast scale of big data, which makes achieving "meaningful consent" nearly impossible. Entities typically secure users' consent through privacy policies, but these policies are often long, complex, and filled with technical jargon. As a result, users frequently fail to fully understand the terms, and their consent may not be genuine. Another issue is the unavoidable sharing of personal information in the digital age. The widespread reliance on online services, the unequal power dynamic between users and entities, and the high costs of finding alternatives make it difficult for individuals to avoid sharing their data. This means that users often have little choice but to consent, even when they are uncomfortable with the terms. In many cases, users do not even read privacy policies, instead agreeing automatically to access services. These problems highlight the failure of the informed consent framework to give users true control over their personal data. It is clear that relying solely on informed consent cannot address the complexities of modern data processing. Given these challenges, paternalistic legislation offers a possible solution. The *American Privacy Rights Act of 2024* (APRA) provides a good example by introducing a "data minimization" approach, marking a shift in U.S. privacy law. Historically, the U.S. used an opt-out system, where users had to actively refuse data processing. This system, like informed consent, was designed to allow individuals to manage their own personal data but has proven ineffective in practice. The APRA adopts a different approach, limiting data collection to only what is strictly necessary for specific and clearly defined purposes. This prevents entities from collecting excessive or unnecessary data from the outset. Furthermore, the APRA strengthens transparency by requiring entities to provide clear and accessible information about their data practices. It also imposes strict obligations on entities and uses advanced technology to reduce the risk of misuse. These measures collectively safeguard users' privacy, even without relying heavily on users' consent. However, the shift to paternalistic legislation is not without risks. While it promotes data autonomy and ensures better privacy protection, it might not fully address diverse users' needs. To balance these concerns, China could explore a "minimized informed consent" framework, which combines elements of both informed consent and paternalistic principles. This framework could involve three main components. First, the scope of minimized informed consent should be clearly defined and gradually expanded. Entities would only be allowed to process personal data that is strictly necessary for providing specific services or products. Second, transparency requirements should be strengthened in two ways: through simplification and refinement. Simplification means making privacy policies shorter, clearer, and easier for users to understand, while refinement involves specifying detailed notification obligations, ensuring users can easily withdraw consent at any time. Third, pilot programs for privacy-enhancing technologies could be introduced to balance the protection and practical use of personal data. By adopting such a framework, China could address the limitations of the current informed consent model while ensuring that users' privacy is protected in a practical and balanced way.

Key words: personal information; informed consent; APRA; paternalism; data minimization