

无需实质同意：同意规则的形式化及其功能

张 鼎

摘 要：作为个人信息处理规则的同意规则在实践中表现为形式化。形式化的同意规则具有规范启示意义。既有理论将同意规则的制度目标建构为追求个人实质同意保障个人自决权，但由于信息主体的认知状态、决策的制度结构约束、信息流动的关系属性，信息主体作出实质同意的可能性较小，追求实质同意的制度目标与制度现实存在差异。形式化的同意规则衍生出意外的制度功能，包括为作为信息处理的避风港、信息监管的传声筒、信息信任的脚手架。形式化同意规则的制度功能与制度优势表明无须废除同意规则，对同意规则的改造需要舍弃实质同意，围绕形式化同意规则重新认识与建构同意规则。具体的规范建构包括：将同意规则改造为信息处理行为必须经历的前置性程序；将同意规则的规制重心转变到保护信息主体的实质不同意决策；区分同意规则的事前面向与事后面向。

关键词：形式化同意规则；个人信息处理；实质不同意；信息信任

〔中图分类号〕D922.8 〔文献标识码〕A 〔文章编号〕2096-6180（2025）05-0044-21

引言

《中华人民共和国个人信息保护法》（下称《个人信息保护法》）第13条第1款第1项将“取得个人的同意”作为个人信息处理的前提条件；征求个人同意也可以见诸其他有关个人信息处理的法律规定中，本文将这些规则简称为“同意规则”。在理论上，同意规则是《个人信息保护法》的基本规则^{〔1〕}，以信息主体的实质同意作为个人信息处理的前置要件，其理论基础包括个人对个人信息的自决权与个人意思自治^{〔2〕}。相对地，同意规则在实践中流于形式，信息主体极少作出同意规则预期中的实质同意决策。基于此，如何理解同意规则实践与理论的差异，又应当如何调整同意规则及其理论？

〔作者简介〕张鼎，法学博士，西南财经大学法学院讲师。

〔1〕程啸：《论我国个人信息保护法中的个人信息处理规则》，载《清华法学》2021年第3期，第62页；王俏：《个人信息保护法：构建以告知—同意为核心的处理规则》，载《人民法院报》2021年8月21日，第1版。

〔2〕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，第2页。

对此，既有的研究已有充分讨论。一些观点认为应当坚持同意规则的法律地位并采取优化措施以实现实质同意。^{〔3〕}但由于仍以实质同意为制度目标，对同意规则的优化措施未能弥合理论与现实之间的矛盾与差异，优化措施仍然流于形式。有意思的是，优化论多出现在《个人信息保护法》出台之前，在《个人信息保护法》出台之后，大量的研究不再聚焦于优化告知同意的方式，而是思考是否可以弱化同意规则^{〔4〕}，或者提炼同意规则的制度功能并重新设计同意规则^{〔5〕}。尽管论证思路与具体规范构造存在差异，但这些研究分享共同的认识——同意规则的实质化目标难以实现，应当在形式化同意规则的基础上重构同意规则。

就“行动中的法”而言，书本中追求实质同意的同意规则的形式化已经是不可避免的现实。即便采取强制阅读、动态一分层同意、分级一分段一分类同意^{〔6〕}，信息主体仍然会作出形式化的同意决策；即便少数个体会审慎地作出实质同意，但多数个体仍会选择形式化同意。信息主体未必认为作出同意是一项权利^{〔7〕}，更有可能认为作出同意是获得网络服务的法律程序要求。因此，既然实质同意无法达成，不妨坦然接受同意规则的形式化并从理论与规范上将其彻底形式化。将同意规则形式化并不会降低法律对个人信息的保护水平，个人信息保护水平与国家对个人信

一、同意规则的形式化

法律理论在建构同意规则时以追求实质同意为制度目标，但追求实质同意的制度目标并未实现，同意规则在实践中流于形式。基于认知心理、制度结构、信息流动关系的分析表明，同意规则的形式化是不可避免的。因此，可行的理论思路是基于信息流动实践重构同意规则。

（一）实质化目标与形式化现实

同意规则追求信息主体在充分告知与有效知情下自主决策作出实质同意。首先，同意规则将信息流动与处理的决策权配置给法律拟制的信息主体，认为信息主体能够基于其自由意志作出选择。其次，为了让信息主体能够基于个人理性作出决策，信息处理者应当充分告知信息处理的方

〔3〕 宁园：《个人信息保护中知情同意规则的坚守与修正》，载《江西财经大学学报》2020年第2期，第116页；郑佳宁：《知情同意原则在信息采集中的适用与规则构建》，载《东方法学》2020年第2期，第205-207页。

〔4〕 向秦：《论个人信息处理中个人同意的“弱化”与信义义务的“补充”》，载《法律适用》2022年第11期，第58页；廖丽环：《个人信息处理中同意规则弱化适用的路径优化——基于情境脉络完整性理论的场景细分》，载《法制与社会发展》2022年第6期，第156页。

〔5〕 罗寰昕：《隐私政策的过去、现在和未来：从合同、基准到信任背书》，载《南大法学》2023年第5期，第103页。

〔6〕 廖丽环：《个人信息处理中同意规则弱化适用的路径优化——基于情境脉络完整性理论的场景细分》，载《法制与社会发展》2022年第6期，第72-178页。

〔7〕 向秦：《论个人信息处理中个人同意的“弱化”与信义义务的“补充”》，载《法律适用》2022年第11期，第60页。

式、信息收集的范围、可能产生的风险等。再次，除了法定情形之外，未经同意的个人信息处理会面临法律制裁，轻则应用下架、约谈整改，重则行政处罚、刑事制裁。最后，同意规则会基于信息性质差异设置不同形式的同意规则，比如要求敏感个人信息的信息处理必须获得明示同意，就不同场景的信息设置差异化的告知与获取同意方式。⁽⁸⁾

相较于同意规则的实质化目标，同意规则在信息处理实践中已经流于形式。形式化的同意规则主要表现在告知、同意两个方面。在信息处理者告知方面，在监管要求下⁽⁹⁾，信息处理者基本均会征求信息主体的同意并发布形式完整的隐私政策，部分互联网企业还会采取动态同意、撤回同意等措施以满足法律的要求。形式完备的告知手段导致信息主体必须作出形式同意以获取信息网络服务。在信息主体同意方面，信息主体极少会作出不同意决策、几乎不阅读隐私政策、不行使同意规则赋予的权利。一些媒体调查表明大量受访者不会阅读隐私政策，信息主体在获取信息网络服务时会直接选择同意信息收集。⁽¹⁰⁾司法实践同样可以表明同意规则流于形式，提出三重同意（授权）的微博脉脉案并非因为信息主体未能作出实质同意，而是因为微博与脉脉的商业竞争⁽¹¹⁾；判决强制同意无效的携程大数据杀熟案的直接动因是携程用户认为其遭受了价格歧视，案件的实际争议点与法律争议点存在偏差，同意规则并未成为实际争议点⁽¹²⁾；或许正是因为案件稀少，一些涉及同意规则细枝末叶的案件也被作为典型案例。

形式化的同意规则同样体现在法律对数字经济的影响中。研究者预测追求实质同意的同意规则将会增加大数据产业的成本。⁽¹³⁾但是信息产业并没有因为同意规则的设立而受到影响，基于数据收集、处理、分析的人工智能产业也正处于迅猛发展之际；相较于同意规则，数据产业更受到数据孤岛、数据质量、数据安全、数据交易基础设施等问题影响。⁽¹⁴⁾更具体的例子则是，有学者认为要求通讯录信息收集需要获得信息主体同意将会对社交媒体带来毁灭性打击，但其所引用案例涉及的社交媒体在相关法域运营良好。⁽¹⁵⁾另一悖论之处在于，尽管《个人信息保护法》第13条为了便利信息产业的发展设置了无需同意的情形，但诸多信息处理者仍然会将第13条无需同意

(8) 《信息安全技术 个人信息处理中告知和同意的实施指南》，GB/T 42574-2023。

(9) 方正梁：《工信部持续开展 APP 治理 行业生态改善成效显著》，载《人民邮电报》2023 年 10 月 27 日，第 2 版。

(10) 王品芝、肖平华：《“我已阅读并同意”？七成受访者坦言很少或从没阅读过 App 用户协议》，载《中国青年报》2022 年 3 月 31 日，第 10 版；光明日报与武汉大学联合调研组：《保障安全的“权利书”，还是窃取信息的“任意门”——App 隐私协议现状调查》，载《光明日报》2021 年 8 月 19 日，第 7 版。

(11) 北京市海淀区人民法院民事判决书，（2015）海民（知）初字第 12602 号。

(12) 浙江省绍兴市中级人民法院民事判决书，（2021）浙 06 民终 3129 号。

(13) 田野：《大数据时代的知情同意原则的困境与出路——以生物资料库的个人信息保护为例》，载《法制与社会发展》2018 年第 6 期，第 118 页。

(14) 谭睿鹏：《系统布局数据基础设施建设》，载《经济日报》2025 年 5 月 23 日，第 5 版。

(15) 韩旭至：《个人信息保护中告知同意的困境与出路——兼论〈个人信息保护法（草案）〉相关条款》，载《经贸法律评论》2021 年第 1 期，第 50 页；有关其分析的中国香港、德国 WhatsApp 的市场状况，分别参见 *Penetration Rate of Leading Social Media Platforms in Hong Kong as of 3rd Quarter 2024*, <https://www.statista.com/statistics/412500/hk-social-network-penetration/>; *Whats App Penetration Rate in Selected European Countries in 3rd Quarter 2024*, <https://www.statista.com/statistics/1005178/share-population-using-whatsapp-europe/>。

的情形加入隐私政策中征求信息主体同意。以上情况说明，实践适用中的同意规则无需信息主体的实质同意，同意规则流于形式化。

主张同意规则的学者未必没有意识到同意规则不可避免的形式化现实。比如，有观点认为不应当将《个人信息保护法》中的同意规则作为民法学说上的意思表示，即信息主体作出的知情同意决策不产生达成合同所需的合意效果；知情同意仅仅只是一种法律上的行为，产生区分合法与非法的标准。^{〔16〕}更确切地说，同意规则设定的“取得个人的同意”不以“有效知情、理性决策”为必要条件，个人同意这一外观即可作为“取得个人的同意”有效的充分条件。

（二）形式化同意规则的成因分析

同意规则为何形式化？是否可以避免同意规则的形式化？诸多研究已经指出同意规则在法律实践中的困境及其原因。^{〔17〕}概括而言，这些研究认为信息主体的认知缺陷、法律工具的不当设计导致了同意规则的形式化。尽管此类研究有着详实的材料与因果分析，但由于未能深入解释形式化同意规则的运行机制及其内在矛盾，这些研究仍以实质同意为制度目标。对形式化同意规则的成因分析表明可行的思路是应当舍弃实质同意，有必要在现有规则的基础上构建形式化的同意规则。

1. 信息主体的认知状态

基于认知状态的解释从信息主体的决策能力出发，认为知情同意过程披露中隐私政策设置的阅读障碍和信息收集与处理涉及的技术复杂性会增加认知压力。基于认知状态的解释存在解释循环，其假定形式同意是非理性决策的结果，但解释者在解释时提前设定了理性决策范本。

借助心理学，可将已有研究重新归类。基于信息主体认知状态的不同，可将认知状态分为信息过载与认知操纵。信息过载指的是当信息的量超过最佳决策所需时，增加信息反而会降低决策主体的决策产出。^{〔18〕}在告知同意场景中，冗长的告知内容、复杂的法言法语都可能导致信息过载，这些难以理解的隐私政策频繁出现在人们的日常生活中。过量、复杂、频繁的信息导致信息主体在知情同意决策过程中面临信息过载。此外，信息处理者可能会通过暗黑模式、利用认知错误、分散注意力、干扰等方式操纵信息主体的认知。^{〔19〕}法律不可能改变信息主体的认知能力，

〔16〕 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43页。

〔17〕 有关参考文献主要为：田野：《大数据时代的知情同意原则的困境与出路——以生物资料库的个人信息保护为例》，载《法制与社会发展》2018年第6期，第117-119页；韩旭至：《个人信息保护中告知同意的困境与出路——兼论〈个人信息保护法（草案）〉相关条款》，载《经贸法律评论》2021年第1期，第48-50页；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89-92页；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38-40页；Neil Richards, Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 Washington University Law Review 1461, 1478-1491 (2019).

〔18〕 Miriam Arnold, Mascha Goldschmitt & Thomas Rigotti, *Dealing With Information Overload: A Comprehensive Review*, 14 Frontiers in Psychology 1, 2 (2023).

〔19〕 Jamie Luguri, Lior Jacob Strahilevitz, *Shining A Light on Dark Pattern*, 13 Journal of Legal Analysis 43, 48-58 (2021).

因此大量研究试图通过优化信息主体的认知环境补救同意规则，如动态同意⁽²⁰⁾、隐私政策标签化等。然而，动态同意与隐私政策标签化的效果有限。事实上，即便在医疗数据领域，动态同意的效果也仍然受到同意疲劳（consent fatigue）的影响。⁽²¹⁾ 隐私政策标签化在实验室中会显著改变隐私决策⁽²²⁾，但实验室外的效果仍然面临诸多挑战，而信息主体的认知状态仍是主要问题⁽²³⁾。

认知心理解释能够展现信息主体的认知心理状态，但更能说明同意规则的内在矛盾。其一，充分告知与有效认知的矛盾。⁽²⁴⁾ 信息收集与使用过程中的认知同意决策需要在宽松的环境中作出，而人们本就会排斥过多信息。⁽²⁵⁾ 但征求同意所处的信息交互环境往往需要信息主体迅速作出决策；同时，信息主体还需要认知与判断信息交互之外的事件，比如了解某 App 的使用方式、资金去向、如何获得服务等。可见，信息主体在知情同意过程中面临充分告知与有效认知之间的结构性矛盾。其二，整体认知与具体同意的矛盾。信息主体对信息交互的认知并非认知交互过程而是交互界面，即信息主体会将同一信息服务的不同服务板块、不同的信息收集与处理过程认知为一个整体。⁽²⁶⁾ 其三，以认知状态作为解释变量看似是以认知科学为依据，但是却未能脱离对实质同意的追求，仍将个人理性与自由意志作为信息流动的阀门。因此，由此展开的研究始终如何获取个人实质同意为制度目标。概括而言，同意规则的内在矛盾是同意规则要求的有效告知与信息主体的有限认知之间的矛盾。

2. 决策的制度结构

认知心理解释尽管能说明同意规则的内在矛盾，但即便信息主体能够作出同意规则所假定的完美认知决策，同意规则仍然有无法调和的内在矛盾。与同意规则相关联的各种正式规则与非正式规则构成了信息主体决策的制度结构，这是信息主体难以突破的结构性约束。

不同意决策的后果将约束信息主体的决策，而法律无法有效调节。在诸多信息交互场景中，若信息主体作出不同意决策，其将无法获取相应的信息网络服务，而诸多信息网络服务已经成为人们数字化生活的必备乃至基础设施，比如地图导航需要获取精确的地理位置信息。法律的应对措施包括：将某些信息设置为无需同意便可处理的信息，取消征得同意环节，比如“订立合同所

(20) 田野：《大数据时代的知情同意原则的困境与出路——以生物资料库的个人信息保护为例》，载《法制与社会发展》2018年第6期，第125页。

(21) Winnie Lay et al., *A Rapid Review of the Benefits and Challenges of Dynamic Consent*, 21 *Research Ethics* 180, 196 (2025).

(22) Patrick Gage Kelly et al., A “Nutrition Label” for Privacy, in SOUPS’09: Proceedings of the 5th Symposium on Usable Privacy and Security 2009, Article No. 4.

(23) Shikun Zhang et al., *How Usable Are iOS App Privacy Labels?*, 4 *Proceedings on Privacy Enhancing Technologies* 203, 218–219 (2022).

(24) 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92页。

(25) Dan Svirsky, *Privacy and Information Avoidance: An Experiment on Data-Sharing Preferences*, 51 *The Journal of Legal Studies* 63, 63 (2022).

(26) 重庆市第一中级人民法院民事判决书，（2021）渝01民终7883号。该案中，在原告请求中，原告作为信息主体指出其通过微博借钱作出同意决策时并没有区分提供交互页面的微博与实际借款人微聚之间的区别，并且也没有区分借款人与其他催收主体的区别，而是将上述信息处理者作为整体。

必须”；以最小必要原则应对。⁽²⁷⁾但“订立合同所必须”与最小必要原则本就难以说明界定，甚至司法实践更有可能以不构成最小必要原则拒绝支持信息主体的不同意决策，在携程大数据杀熟案中，二审法院便以此种理由拒绝了信息主体的请求。⁽²⁸⁾不同意决策的后果说明了同意规则的另一内在矛盾：同意规则预设了个人自由意志与理性决策，但自由意志与理性决策并非法律规定就能够赋予的；当持有、行使权利的成本超过相应的收益后，法律赋权就会被权利人搁置。同意规则并不能解决这一内在矛盾，因此实践中的同意规则逐步形式化。

此外，法律对不同意后果的干预具有复杂的经济后果。在携程大数据杀熟案中，一审法院认为携程通过信息收集进行用户画像超出了最小必要原则，因此支持胡女士提出的“不同意仍可使用”的请求。二审法院却认为数字经济长远发展需要创新，因此不应过分苛责携程。对比两级法院的不同意见，可以发现法院对不同意后果的干预是在干预商业模式。法律对商业模式的干预必须保持足够谨慎，而其涉及合法性问题则将牵涉经济法。尤其是，对于不同规模的公司，干预的后果可能并不均等。法律面前，公司与公司并不平等。一种可能的后果是，法律干预将增加小型、专业化的公司的竞争劣势，扩大大型、通用型平台公司的竞争优势。这可能是因为个人信息保护法律对小型、初创公司的合规成本与要素成本的边际影响更大。

3. 信息流动的关系属性

以实质同意为目标的同意规则将信息流动过程理解为授权—获权的过程，将同意规则可能涵射的信息理解为天然存在有待采撷的资源。这种思路未能理解信息的关系属性，信息并非孤立之物，信息嵌入社会关系与经济关系中。信息是人们社会互动的产物，诸如互联网上的昵称、头像与行为数据产生于人们使用网络服务的过程中，嵌入在用户—网络服务提供者这对关系之中。即便是姓名、身份证号这些更具有个人专属性、人格属性更强的信息，对其功能的理解也需要定位至具体的关系中⁽²⁹⁾，这类身份认证信息是人们参与社会互动的基本标识。同意规则设定的授权—获权过程并没有考虑信息的关系属性。

信息的关系属性决定个人信息不可能依照“实质同意”的方式流动。其一，产生于关系中的信息具有双边性，关系中的双方均可以主张对信息的权利，比如就认证信息而言，公众可以主张识别权，认证信息主体可以主张禁止滥用。⁽³⁰⁾其二，信息的关系属性表明信息与信息之间具有关联性。当某人的信息被收集之时，与之关联的他人信息也可能被收集，比如通讯录信息、购物信息中包含的他人购物偏好等。博弈论分析表明，信息的关联性将导致人们始终作出同意信息收集的决策。⁽³¹⁾信息的关系属性意味着追求实质同意的同意规则存在根本性的内在矛盾，同意规则必

(27) 武腾：《最小必要原则在平台处理个人信息实践中的适用》，载《法学研究》2021年第6期，第74页。

(28) 浙江省绍兴市中级人民法院民事判决书，(2021)浙06民终3129号。

(29) 胡凌：《功能视角下个人信息的公共性及其实现》，载《法制与社会发展》2021年第5期，第183页。

(30) 高富平：《个人信息保护：从个人控制到社会控制》，载《法学研究》2018年第3期，第95—96页。

(31) Daron Acemoglu et al., *Too Much Data: Prices and Inefficiencies in Data Markets*, 14 American Economic Journal: Microeconomics 218, 219 (2022).

然会在法律实践中演变为形式化的规则。

上文分析表明,由于同意规则的内在矛盾,同意规则在实践中将会转变为形式化规则,追求实质同意的同意规则将会失效。直观上,信息主体的认知偏差是信息主体无法作出实质同意的原因。然而,即便信息主体能够作出完美决策,信息主体决策所嵌入的制度结构也不支持信息主体作出不同意决策。但是,即便制度偏袒信息主体,信息的关系属性也意味着信息主体无法作出实质同意,其对于信息流动的流向与可能后果无法控制。对同意规则形式化成因的分析还表明,同意规则的形式化在法律适用中是无法避免的客观现实。若法律理论坚持以实质同意作为制度目标,对同意规则的调整不仅不会增加信息主体作出实质同意的可能,反而还可能会增加其认知负担与决策负担,导致信息主体更容易被操纵。比如,部分信息处理者借助暗黑模式,诱导用户在动态一分层同意中勾选付费服务,而该机制本用于保障实质同意决策。

二、形式化同意规则的功能及其制度优势

同意规则的形式化并不意味着需要废除同意规则。尽管同意规则未能促成实质同意,但在法律实践中却衍生出意外功能。意外功能的存在表明有必要保留形式化的同意规则,对意外功能的分析还将说明相较于实质同意,形式化的同意规则更具制度优势。丁晓东总结了同意规则的数项意外功能:自我规制的章程、声誉机制的媒介、法律实施的依据、沟通教育的工具。⁽³²⁾其总结不无道理,但仍有不足,诸如自我规制、沟通交流等功能被过于理想化,这是因为他引用的美国法与中国法存在差异,美国法将隐私政策理解为合同⁽³³⁾,但中国法理论并不认为告知同意等同于合同合意⁽³⁴⁾。相较于各类法律法规、标准指南,隐私政策作为执法依据的效力较弱。声誉机制在国外或成立,在中国并没有专门机构评测;但即便有评测,评测结果的影响也较小;有效的声誉机制事实上与实质同意一般,当同意规则形式化之后,声誉约束也将失效;事实上,尽管工信部已经公布了多批次的个人信息处理违法 App 清单,但其声誉效果极为有限。这部分结合已有的研究与其他经验,将同意规则的功能总结为信息处理的避风港、信息监管的传声筒、信息信任的脚手架。三个意外功能分别对应同意规则的三个面向:信息收集者、监管者、个体。

(一) 信息处理的避风港

作为一种法律技术,避风港规则指的是“权威机关在相对原则、一般的行为限制和追责体制下,以具体规则的形式,为受法律约束的社会行为主体指明有限、有条件的合规路径的一种法律技术;当行为主体选择在安全港范围内开展相关活动时,便可获得较为确定的免于被追究违法责任的预期”。⁽³⁵⁾在信息处理风险规制体系下,形式化的同意规则相当于为信息处理行为设置了有

(32) 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24页。

(33) Daniel J. Solove, Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Columbia Law Review 583, 595 (2011).

(34) 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43页。

(35) 戴昕:《作为法律技术的安全港规则:原理与前景》,载《法学家》2023年第2期,第33页。

条件的合规要求，当信息处理者实施了征求同意这一行为后便可获得有限的免责预期。

以涉及同意规则的诉讼为例，信息处理者实施告知同意可以降低信息处理行为的法律风险，扩大免责范围。可以将司法实践中关于同意规则的案例分为两类：一类案件只涉及同意的形式问题（Ⅰ类）；另一类案件涉及信息处理的后果并因此要求设置更精致的同意规则（Ⅱ类）（关于两类案件的案情梳理与分析见表 1^{〔36〕}）。在Ⅰ类案件中，信息处理者设定的告知同意形式可以避免信息处理行为遭受法律风险，比如芝麻信用案、阿里妈妈评分案；当信息处理者未能履行告知同意的法律形式时，无论其行为性质如何，信息处理行为都将被评判为违法，比如线下门店消费信息案、流行语词典案。在Ⅱ类案件中，司法裁判表现为责任规则^{〔37〕}，信息处理行为的法律风险将基于信息流动的性质评判。信息处理行为有可能会被认为合法，即便信息处理行为被认定为侵权，其法律后果通常仅为要求改进同意规则的形式以及极低的赔偿，如朱某诉百度案、数据跨境流动案、携程大数据杀熟案。

表 1 司法实践中关于同意规则的两类案件

类型	案名	案情	法律问题
Ⅰ类案件	芝麻信用案	芝麻信用平台采集用户的执行案件信息被用户起诉侵权	取得用户的同意后是否可以收集案件执行信息
	线下门店消费信息案	未征求同意，消费者使用扫一扫支付被收集线下购物信息	未获得形式同意收集信息是否违法
	流行语词典案	一款提供流行语词典的移动应用未经用户许可自动勾选同意	自动勾选同意是否可以被认定为有效同意
	阿里妈妈评分案	阿里妈妈通过收集 Cookie 发现网站异常流量	概括同意后是否可以收集 Cookie
Ⅱ类案件	朱某诉百度案	百度基于朱某上网的 Cookie 记录以弹窗形式推荐“减肥、丰胸、人工流产”广告	弹窗“减肥、丰胸、人工流产”是否会有损尊严
	数据跨境流动案	注册国际酒店会员后，个人信息未经单独同意被传输至多个国家	个人信息跨境流动是否需要征求单独同意
	携程大数据杀熟案	携程基于用户的消费记录设定不同的价格	网络平台是否有权实施基于用户数据的价格歧视
	豆包搜索案	可以通过生成式人工智能搜索出个人的姓名、身份证、微信号、学号等信息	生成式人工智能是否可以输出整合后的个人各类身份信息

〔36〕 杭州互联网法院民事判决书，（2018）浙 0192 民初 302 号；流行语词典案与线下门店消费信息案，《北京互联网法院涉个人信息及数据典型案例》，载微信公众号“北京互联网法院”2024 年 10 月 31 日，<https://mp.weixin.qq.com/s/500PiHzTPl3VZ9Vg75lbwg>；浙江省杭州市中级人民法院民事判决书，（2018）浙 01 民终 7505 号；江苏省南京市中级人民法院民事判决书，（2014）宁民终字第 5028 号；广州互联网法院民事判决书，（2022）粤 0192 民初 6486 号；浙江省绍兴中级人民法院民事判决书，（2021）浙 06 民终 3129 号；《大厂 AI 能问出个人微信号？实测各大模型“吞吐”个人信息》，载微信公众号“竞争秩序场”2024 年 12 月 12 日，<https://mp.weixin.qq.com/s/LkMadfykVtAr7e7O9LzXSg>。

〔37〕 张鼎：《数字要素流动的责任规则：实践与原理》，载《甘肃政法大学学报》2024 年第 1 期，第 78 页。

I类案件与II类案件的区别分别对应同意规则作为避风港规则的双重制度功能。I类案件中涉及的同意规则形式问题表明在法律形式上,同意规则提供了区分合法信息流动与非法信息流动的符码。诸如内部人泄露、计算机系统后门等非法个人信息流动均不可能有形式上的同意规则,换言之,计划以合法方式处理个人信息的主体可以通过履行最低限度的告知同意将其与非法处理个人信息相区分。信息处理者告知同意行为会产生自我设限的后果,即唯有落入隐私政策文本中的信息处理行为才会被认定为合法;若信息处理者私自“留后门”,其行为将被判定为违法。当然,不应当期待隐私政策文本可以穷尽说明信息采集后的处理方式、流动方式、流动对象以及使用方式。因为法律需要鼓励信息处理者发现有价值的信息互补性,而详尽的告知同意规则可以通过II类案件事后细化。

作为法律技术的避风港规则仅提供有限的免责预期,同意规则也并非是为信息处理行为提供无限豁免能力的金钟罩。信息处理行为总会带来一些新的规制场景,法律必然无法事前穷尽具体的信息处理行为以及详尽的告知同意规则。因此,必须设置原则性的方案为经济行为提供免责空间与事后评价的可能性。在II类案件中,新的信息处理方式、流动途经产生的社会风险已经出现,比如数据跨境流动可能扩大数据风险、朱某诉百度案中朱某的尊严性隐私未能得到保护;法律的回应方式可能是关于同意规则的,即要求改进告知同意规则,比如数据跨境流动案要求征求单独同意。法律的回应也可能会评价信息处理行为,比如携程大数据杀熟案中的价格歧视问题、豆包搜索案中人工智能对信息整合的风险问题。最后,有限的免责预期还能够激励信息处理者减少信息收集的范围,非必要的信息收集、更明确的获取形式同意的方式都将扩大免责空间,而以上功能并不以实质同意为前提。

同意规则的形式化相对于实质化更具有制度优势。就提供的免责空间而言,若将同意规则中的同意定性为实质同意,那么实践中的同意规则在法律逻辑上将会产生绝对的违法阻却效果;相对地,形式化的同意规则并不产生绝对的违法阻却效果^{〔38〕},其提供的免责预期并不会完全豁免信息处理行为。于司法实践而言,形式化的同意规则意味着法院在I类案件中仅需要关注信息处理者是否获得了形式同意,无须耗费司法资源探明信息主体是否作出实质同意,法院因此可以将更多的注意力置于分析II类案件中的利害关系与优化同意规则的形式。因此,就同意规则作为信息处理的避风港规则而言,更适宜采取形式化的同意规则。

(二) 信息监管的传声筒

同意规则避风港功能的实现需要信息传递,告知同意过程中披露的隐私政策将个人信息监管法律作为信息传输给信息处理者,这是形式化同意规则的传声筒功能。传声筒功能通过执法传输、守门人传输两重机制实现。由于传声筒功能,个人信息保护的基准得以设定与执行^{〔39〕},但更严格

〔38〕 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43页。

〔39〕 关于隐私基准,参见罗寰昕:《隐私政策的过去、现在和未来:从合同、基准到信任背书》,载《南大法学》2023年第5期,第110页。

的个人信息流动限制无法通过传声筒实现，仍需要其他制度配合。

1. 执法传输机制

执法过程不仅是法律执行过程还是法律与政策传输至执法对象的过程。传统基层执法面临信息损耗问题，一方面违法信息与具体的执法情况无法向上传递，另一方面抽象的法律法规与政策无法传递至执法对象甚至基层执法者。^{〔40〕} 个人信息执法面临同样的问题。其一，个人信息监管涉及的法律与政策种类多、层次多、领域多、规则细节多^{〔41〕}，法律信息传输的损耗加剧。其二，隐私监管与执法压力巨大。截至 2023 年夏，我国监测到的活跃 App 已多达 260 万款^{〔42〕}；而 App 更新、网页、小程序、线下场景又会进一步增加监管压力，监管机构可投入的监管资源有限。其三，传统执法体系中的层级条块问题以新的方式出现，网络辐射全国，执法仍旧属地管辖，本地执法者的执法动力与能力减弱，执法效果大打折扣。

告知同意过程中披露的隐私政策能够部分解决执法信息损耗问题。首先，由于可以通过互联网直接抽查发现告知同意的履行状况、线上获取隐私政策文本，工信部可以通过直管的方式替代属地管辖，属地部门则基于实际情况开展监管工作。^{〔43〕} 其次，执法部门以技术治理方式监管信息处理行为。工信部在监管活动中通过第三方技术监测、自建 App 技术检测平台的方式发现不合规行为。^{〔44〕} 最后，通过分布式决策弥补执法资源不足的问题，即信息主体通过投诉举报的方式将信息服务互动过程中发现的违法行为报告至监管者。在上述过程中，告知同意所披露的隐私政策文本及其实施情况成为重点监管内容，信息处理者因此会尽可能满足信息监管要求。

2. 守门人传输机制

移动互联网已经成为信息产业的主要信息来源，分发移动应用的应用平台成为个人信息监管的守门人。相比于通过网页收集信息，移动应用一方面收集更多的信息，另一方面也更依赖应用分发平台。在过去的十数年间，各手机厂商、第三方平台建立了多个应用分发平台。随着诸如鸿蒙这类系统拓展至电脑端，应用分发平台的规制范围也随之拓展。应用平台在应用上架审核中会审查信息处理者采取的个人信息保护措施，包括是否设置告知同意、是否制定隐私政策、隐私政策文本与信息处理行为是否相符。通过应用平台的审查行为，个人信息监管法律被传输至信息处理者，个人信息处理合规成为应用上架的前提。

无论是出于商业竞争，还是满足法律对应用平台的监管需求，应用平台客观上扮演了个人信息监管守门人角色。法律学者将守门人概念引入互联网治理中，认为平台应当承担部分监管

〔40〕 刘杨：《执法能力的损耗与重建——以基层食药监执法为经验样本》，载《法学研究》2019 年第 1 期，第 25 页。

〔41〕 关于个人信息保护规范体系，参见程啸：《我国已建立体系比较完整、内容比较具体的个人信息保护规范体系》，载“清华法学院”官网 2024 年 5 月 13 日，<https://www.law.tsinghua.edu.cn/info/1036/19820.htm>。

〔42〕 《我国互联网普及率达 76.4%》，载《人民日报》2023 年 8 月 29 日，第 1 版。

〔43〕 《工业和信息化部关于开展 APP 侵害用户权益专项整治工作的通知》，工信部信管函〔2019〕337 号。

〔44〕 《工业和信息化部关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》，工信部信管函〔2020〕164 号。

职能,履行审查义务。⁽⁴⁵⁾网信办早在2016年就要求应用平台督促应用程序保护个人信息;在2022年则直接规定应用商店应当承担移动应用上架审核与管理义务。⁽⁴⁶⁾在监管要求之外,应用商店为了获得竞争优势也可能会主动审查,如手机厂商为了销售手机会积极推出各类隐私保护措施制约移动应用。应用平台审查移动应用与传播学中的守门人并无二致,如同“投稿一发表”般,应用平台会编辑控制发表质量,将那些不合规的移动应用隔离于消费者。具体而言,应用平台通过“提示信息处理不合规行为、传输合规的信息处理方式”两种方式发挥守门人功能。

应用平台会将抽象的告知同意规则转变为应用平台明确的审核标准,并在具体的审查行为中提示应用程序不合规的信息处理行为。由于应用程序的功能、技术原理、数据需求千差万别,应用平台只能制订大致的审核标准明确信息处理方式,因此应用程序基于同意规则披露的隐私政策成为重要的审查依据。应用平台通常会首先审查隐私政策文本的合规性,若隐私政策明显不合规,应用程序则无法上线。通过隐私政策审核后,应用平台会测试信息处理行为与隐私政策文本的一致性,部分应用程序会因此被拒绝上架。通过技术检测,应用平台能够发现隐蔽的信息处理行为,比如发现SDK的信息处理行为并将SDK的信息处理行为告知应用开发者。

应用平台对告知同意与隐私政策的审核能助推应用开发者履行个人信息保护义务。比如,华为应用市场审核指南中明确规定:“应用的隐私政策链接指向的隐私政策应当包含应用程序(包括委托的第三方或嵌入的第三方代码、插件)收集和使用个人信息的目的、方式和范围。”⁽⁴⁷⁾应用平台对小型信息处理者的助推尤为明显。对互联网大平台而言,技术团队与法务团队的有效配合能够将个人信息保护合规要求转变为代码语言,将程序代码转变为隐私协议。⁽⁴⁸⁾但是中小型企业、初创企业、个人开发者的开发人员少、法律知识与经验匮乏,对于此类信息处理者而言,技术论坛与应用平台提供的合规指南成为此类开发者的学习资料、合规路书。比如,小米应用商城为开发者提供隐私专员予以合规指引,一些技术论坛还会提供实现合规要求的代码文件。由于上述机制的运行,同意规则成为信息监管的传声筒。

同意规则的监管传声筒功能说明即便信息主体无法作出实质同意,形式化的同意规则仍然能够起到个人信息保护的效果。正是由于传声筒功能,废除同意规则的论点并不可取;保留形式化的同意规则并且优化传声机制更为可取。相对于实质同意而言,形式同意使得监管部门无须耗费大量监管资源检查信息主体设置的告知同意是否可以获得信息主体的实质同意;监管部门可以将监管重心置于隐私政策的合规性与隐私政策的实施情况上。相较于实质同意,形式同意将更有利于促进个人信息保护。

(45) 祖璐:《“数字守门人”:法理逻辑与中国启示》,载《经济法论丛》2024年第2卷,第378页。

(46) 《移动互联网应用程序信息服务管理规定》(2022年修订)。

(47) 《华为应用市场审核指南》,载Harmony OS网2024年4月11日, <https://developer.huawei.com/consumer/cn/doc/50104#h1-1656069583692-6>。

(48) 胡杨潇潇:《论道科技》,载《亚洲法律杂志—中国版》2020年第11期,第39页。

需要说明的是，传声筒功能不可能完全杜绝违规违法的个人信息处理行为。一项对中国网站行为的研究发现网站实际的信息处理行为与披露的隐私政策存在严重不符。⁽⁴⁹⁾当涉及第三方信息共享时，平均有 89.8% 的网站的数据分享行为与其隐私政策一致，但这是因为其中多数网站在隐私条款上采取了模糊策略，网站并未实际披露其信息共享行为。在信息存储方面，仅有 44% 的网站行为符合其披露的隐私政策，但其中同样有大量网站采取模糊策略，刻意模糊信息存储行为。在上述两种情形中，均有大量网站的行为完全不符合其披露的隐私政策。以上数据说明，隐私政策并不等同于隐私实践，传声筒能够传达信息，但其有效性取决于配套的法律措施。

（三）信息信任的脚手架

同意规则及经由同意规则披露的隐私政策具有增进信任的功能。以数据驱动的平台经济需要建立在用户信任的基础上，用户只有在信任平台信息处理后会才会托付其数据。⁽⁵⁰⁾有研究洞察到“当个人分享信息供他人利用，也信任他人在处理中能够保护其个人信息权益”⁽⁵¹⁾，这是一种普遍的社会信任。这部分的分析将说明，形式化同意规则具有增进普遍社会信任的功能。

在理论上，需要说明信息信任与信义义务之间的关系。美国学者巴尔金提出了个人信息信义义务模型。⁽⁵²⁾信义义务模型认为信息处理者对信息主体负有保密义务、注意义务、忠诚义务。实证研究揭示的信任机制能够丰富信义义务理论。其一，信任机制表明，同意规则能够增进信任，信任的客观存在是信义义务的基础，法律不可能借助信义义务无中生有地创造信任。其二，信息处理者违反信义义务会降低整个产业的信任度，这是法律处罚的原因。其三，信任（trust）不等于信托（trust）。信托是一种有关财产处置与收益的制度工具，信任客观存在于社会关系中，信义义务具有维护并促进信任的功能，而形式化的同意规则相较于信义义务更能促进信息信任。

有研究指出人们在信息互动中同意信息收集的决策存在非理性成分。⁽⁵³⁾非理性决策与信息主体对信息流动的风险和负面后果认知不足有关，但在更普遍的信息流动场景中，信息流动中的非理性决策来自普遍存在的社会信任——由于对信息处理行为的信任，人们不必精于理性算计；当然，如果对信息处理行为普遍不信任，那么人们则会更加倾向于作出不同意的决策。借助社会学对社会信任的分类，可以将信息流动中的社会信任分为关系信任与普遍信任。⁽⁵⁴⁾关系信任指的是信息主体对特定交往主体的信任，比如信息主体对特定社交关系、特定网络平台信息处理行为的信任；普遍信任指的是信息主体对经济社会中整体信息流动后果的信任。正是通过具体信息流动场景中的关系信任与对经济社会中信息流动的普遍信任，基于信息流动的经济发展才能得以繁荣。

(49) Xinjie Lin, Han Liu et al., *Privacy Protection of China's Top Websites: A Multi-layer Privacy Measurement via Network Behaviours and Privacy Policies*, 114 *Computers & Security* 1, 18 (2022).

(50) 戴昕：《平台责任与社会信任》，载《法律科学（西北政法大學學報）》2023年第2期，第84頁。

(51) 向秦：《论个人信息处理中个人同意的“弱化”与信义义务的“补充”》，载《法律适用》2022年第11期，第66頁。

(52) Jack M. Balkin, *The Fiduciary Model of Privacy*, 133 *Harvard Law Review* 11, 11–14 (2020).

(53) 何佳等：《个人信息披露决策：强制收集与挤入效应》，载《经济研究》2022年第5期，第173頁。

(54) 陈福平：《市场社会中社会参与的路径问题：关系信任还是普遍信任》，载《社会》2012年第2期，第86頁。

于法律治理而言，法律的功能并不在于构建信义义务促进信任，而应当是采取措施维护社会信任，同意规则正是其中一环。

在具体的关系信任中，同意规则通过提升信息主体的参与感与满足信息主体的隐私偏好促进关系信任。在消费心理学研究中，研究者发现同意规则可以显著增进信任，降低隐私顾虑。⁽⁵⁵⁾这是因为披露隐私政策不仅增加信息处理透明度，同时也会释放信息安全处理的信号，形式化的同意还会带来参与感与控制感，以上机制的运作并不以信息主体阅读隐私政策为前提。此外，同意规则还能满足人们差异化、敏感的隐私偏好。以朱某诉百度案为例，该案常被用于分析 Cookie 定性问题，但朱某为何起诉？朱某的诉讼与搜索关键词有直接关系，他（或她）搜索了“减肥、丰胸、人工流产”等词汇，此类内容通常为个人不太愿意为他人所知晓的内容，而他人也往往没有知晓的必要。但百度通过个性化推荐导致朱某家庭与单位的电脑均会出现相关的内容弹窗，这无疑会影响朱某本人在真实社会生活中的尊严性隐私。⁽⁵⁶⁾同意规则提供的拒绝信息收集与处理选项为满足隐私偏好留下了空间，这是数据隐私法尊重与保护个体尊严性隐私的应有之义；关系信任也可以从被尊重的感受中获得建构，因此关系信任的要义并非信息主体的实质同意，而是信息处理者征求同意的形式。

相对于具体的关系信任而言，普遍的社会信任更值得法律保护与促进。普遍信任需要多种社会治理措施共同构建，而同意规则是构建普遍信任的脚手架。以携程大数据杀熟案为例，携程对信息流动秩序的破坏并非仅是携程未能获得胡女士的有效知情同意，更在于其采取的信息用途对社会信任的破坏。⁽⁵⁷⁾若以形式化的同意规则要求携程披露信息用途并认定其将信息用于价格歧视为非法将会有助于构建社会信任。在美国，皮尤调查的数据表明由于政府、互联网公司处理个人信息缺乏透明度、提供的隐私政策流于形式，而频发的网络犯罪、棱镜门事件、剑桥分析事件等进一步导致人们对互联网与政府各类信息处理行为的信任显著下降。⁽⁵⁸⁾概言之，通过同意规则披露的隐私政策文本有助于提升信息处理行为的透明度；而通过传声筒落实的个人信息监管措施则会增加人们对隐私政策文本的信任程度。当然，社会信任的建构需要细心呵护，同意规则仅是诸多维护社会信任措施中的一种工具，此类规则的共同目标在于塑造可信可靠的信息流动环境。

(55) 本文主要参考：Kunal Swani et al., *Revisiting Trust and Privacy Concern in Consumers' Perceptions of Marketing Information Management Practices: Replication*, 56 *Journal of Interactive Marketing* 137, 137 (2021); 梁晓丹：《在线隐私政策对消费者提供个人信息意愿的影响机制研究——信息敏感度的调节作用》，载《管理评论》2018年第11期，第97页；Zhao L. et al., *Disclosure Intention of Location-Related Information in Location-Based Social Network Services*, 4 *International Journal of Electronic Commerce* 53, 53 (2012); Heng Xu et al., *Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances*, 12 *Journal of the Association for Information Systems* 798, 798 (2011).

(56) 朱某与北京百度网讯科技有限公司隐私权纠纷上诉案，江苏省南京市中级人民法院民事判决书（2014）宁民终字第5028号。

(57) 戴昕：《平台责任与社会信任》，载《法律科学》2023年第2期，第88页。

(58) *How Americans View Data Privacy*, Pew Research Center (18 October 2023), <https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/>.

以上分析表明，形式化同意规则具有意外的制度功能，这些意外的制度功能解释了为何同意规则在长期形式化的情况下仍然得到适用。从制度成本与制度收益的角度考量，执行同意规则并未显著增加制度运作的成本，但意外的制度功能却导致同意规则已然成为整体性信息流动规制中的关键一环。因此，对同意规则的反思与改造既不应以追求实质同意为目标，也不应以废止同意规则、弱化适用为目标，而应在当前形式化同意规则的基础上进行细微的规范再造，赋予同意规则以“充分告知、有效知情、自主决策”以外的规范内涵。

同意规则的意外功能还表明有必要对同意规则进行形式化重构。形式化同意规则的制度功能与信息主体的形式同意构成同意规则理论与实践的一体两面。正如有论者指出，形式化的同意蕴含着信息主体对国家治理能力的信任^{〔59〕}，而形式化同意规则的各项制度功能实现的机制正是国家治理能力的具体表现。如果没有形式化同意规则的制度功能，信息主体可能会审慎决策，更有可能作出实质不同意的决策，信息主体的实质不同意又会减缓信息经济的发展。事实上，以实质同意作为同意规则的核心将信息主体置于平衡经济发展与个人信息保护的关键位置，但单个的信息主体并没有相应的决策资源与决策能力。形式化的同意规则是当前经济发展与个人信息保护所形成的均衡结果，对同意规则的理论解释应当基于当前均衡结果予以提炼。因此，面对同意规则理论与实践的差异，对同意规则的规范改造有必要将同意规则从理论上彻底形式化。

三、无需实质同意：形式化同意规则的规范构造

前文的分析说明了对同意规则进行形式化重构的必要性，这部分将通过具体的规范构造与解释说明形式化同意规则的可行性。在规范构造上，笔者将同意规则作为信息处理者的前置程序而非基础性规则，将同意规则的重心由追求实质同意转移至保护实质不同意，从事前事后角度区分同意规则的不同面向。相较于已有研究中的各类废止论与优化论，本文的规范构造措施并不要求大幅修改法律与调整法律体系，因此更具操作性与可行性。

（一）作为信息处理前置程序的同意规则

个人信息的流动利用与对个人法益的保护向来是数据隐私法难以平衡的两端，同意规则试图引入个人自主决策解决这对矛盾。就此而言，可以将同意规则理解为信息流动的闸门，获得个人同意后的信息可以进入信息流动利用环节。但正如闸门之于水流一般，闸门的开放不仅取决于水库水位，还取决于下游的防洪排灌安全设施，信息流动与否同样受到信息流动之后的信息安全水平影响。信息安全水平受到信息安全技术能力、法律监管要求的共同影响。比如，大型互联网公司通常更有技术能力、经济激励采取复杂的技术措施维护信息安全，而小型企业、社区、个体工商户等主体则缺少信息安全维护能力。法律还会就不同的数据类型、不同的信息处理者施加不同的要求。另外，信息流动的必要性也将决定信息流动与否。基于信息安全水平、信息流动必要性，

〔59〕 万方：《个人信息处理中的“同意”与“同意撤回”》，载《中国法学》2021年第1期，第168页。

可以将信息流动规范进行以下分类，见表2。

表2 控制信息流动的规范类别

信息安全水平	信息流动必要性强	信息流动必要性弱
信息安全水平高	同意规则+强制流动	（稀有场景；不太可能出现）
信息安全水平弱	同意规则	禁止流动

当信息安全水平要求较高且信息流动必要性强时，法律对信息流动的控制可以采取同意规则与强制性规范。此类规范的典型场景包括大型互联网平台处理用户信息、国家机关处理个人信息等。事实上，《个人信息保护法》第13条第1款第2、3、4项均可被理解为无需同意的强制性规范。在此类规范场景中，信息流动的必要性强，且流动的信息更有可能涉及个人敏感信息、基础性身份信息。为了满足流动需求，法律通常会要求此类信息处理者履行更高的信息安全保护义务，如《个人信息保护法》第58条对提供互联网平台服务、业务类型复杂的个人信息处理者的要求，以及政务数据处理通常有着更为严密的数据安全制度。^{〔60〕}

当信息流动必要性较强，但是信息安全水平较弱时，法律可以采取同意规则将信息流动的决策权交予信息主体。此类规范的典型场景包括各类中小型网络平台或网站提供网络服务、线下场景通过数字化的方式收集信息等。以停车服务场景为例，无人驻守的停车场可以节省大量人工成本，但无人驻守的停车服务需要停车场收集车牌信息乃至手机号、支付信息等，而诸多停车服务提供者并没有完善的数据安全维护能力。^{〔61〕}但是，便捷的车牌识别、迅捷的停车找车过程、顺滑的进出停车场体验又使得信息流动的必要性增强。因此，法律可以将此信息流动的决策权交给信息主体。这就解释了多数网络服务中的信息流动秩序、多种场景中的人脸识别规范：信息主体可以自行决策信息流动状态或者放弃特定信息服务。

在现实的经济社会中，较少出现信息流动必要性弱但是又有着高水平的信息安全水平配套，因而本文不讨论此类场景中的信息流动规范；更为常见也更有意义的是信息流动必要性弱但信息安全水平较低的场景，此类规范的典型场景为扫码点餐、数据跨境流动等。以扫码点餐场景为例，点餐并不需要身份认证，信息流动必要性弱，而餐厅又往往缺乏足够技术实力、资金维护信息安全，其信息安全能力较弱。因此，法律可能会将此类场景中的信息流动规范设定为禁止流动。^{〔62〕}在数据跨境流动场景中，法律要求数据流动必须经过安全评估，这是因为信息流动的必要性随着安全风险的升高而相对降低；若境外接受方的数据保护水平未达到中国法律标准或者说数据安全

〔60〕 苏宇：《政务数据安全的法律制度保障》，载《苏州大学学报（法学版）》2023年第4期，第30-32页。
〔61〕 《停个车，个人信息怎么就泄露了？》，载“澎湃”2025年1月14日，https://www.thepaper.cn/newsDetail_forward_29926132。
〔62〕 陈晓东、雷悦：《扫码点餐录入的个人信息无法自行删除：北京某餐饮公司强制获取消费者个人信息被判承担侵权责任》，载《人民法院报》2023年12月15日，第3版。

被认为未能得到充分保障，法律可能会限制信息流动。⁽⁶³⁾

以上分析说明，同意规则并非个人信息处理行为的基础性规则。同意规则是控制个人信息流动的一种规范类型：在横向维度上，同意规则与禁止性规范、强制性规范共同构成了控制信息流动的闸门；在纵向维度上，同意规则与信息流动必要性、信息安全水平存在关联。

有鉴于此，可以将同意规则重构为信息处理行为必需的前置程序，将同意规则形式化。这是因为同意规则无法在实践中获取信息主体的实质同意，而法律又可以通过信息流动后的安全保障措施控制信息流动的风险与后果，同意规则在实践中又具有制度成本较低的意外功能，所以可将同意规则重构为信息处理的前置程序。论者可能会认为，将同意规则彻底形式化、程序化可能会降低个人对信息流动后果与风险的控制。但上文的分析给出的规范启示在于：如果法律无法提升个人控制对信息风险的控制，那么法律还可以通过增强信息安全保障、控制信息用途等方式实现个人信息权益的保护。⁽⁶⁴⁾ 因此，法律允许平台经营者收集个人信息但是禁止平台将数据用于设定歧视性的交易条件（《个人信息保护法》第 24 条）；金融借贷需要收集个人信息，但是法律对催收中个人信息处理作出了限制。⁽⁶⁵⁾ 这种事后风险控制的思路也是一般化数据风控所采取的方案，比如数据流通交易中采取的“数据可用不可见、用途可控可计量”交易方案。⁽⁶⁶⁾ 正是由于法律可以采取多种事后风险控制机制，同意规则所承载的制度功能才可以由追求信息主体实质同意转变为形式化的信息处理前置程序。

（二）保护“实质不同意”

将同意规则作为前置程序并不等同于不尊重、不保护个人的意愿，而是将同意规则的规范重心由获取信息主体的实质同意转移至保护信息主体作出的实质不同意决策。若将形式化同意规则理解为避风港规则，那么保护实质不同意就是“必翻船规则”⁽⁶⁷⁾——若信息处理者在信息主体作出实质不同意决策后仍然处理信息，其行为必然违法。

同意规则以尊重人格尊严、保障个人自主为法理依据。⁽⁶⁸⁾ 对人格尊严的尊重、个人自主的保护不一定要以“打破砂锅问到底——获得肯定回复”为标准，若信息处理者在告知同意过程中能够减少对信息主体的干扰，将告知同意的重心设置为收集实质不同意决策，其也不失为对信息主体的尊重。另外，不同个体对于隐私与个人信息的敏感程度存在差异，法律既不可能以最敏感者的隐私偏好标准为隐私基准，也不可能以最敏感个体的隐私偏好作为法律锚点。形式化的同意规则因而成为平衡不同隐私偏好的规则工具。对数字经济、信息产业的发展，缺少部分个体的数

〔63〕《数据出境安全评估办法》（国家互联网信息办公室令 11 号），第 8 条。

〔64〕类似思路也被用于论证个人信息的社会控制，参见高富平：《个人信息保护：从个人控制到社会控制》，载《法学研究》2018 年第 3 期，第 100 页。

〔65〕中国互联网金融协会：《互联网金融贷后催收业务指引》。

〔66〕《关于完善数据流通安全治理 更好促进数据要素市场化价值化的实施方案》（发改数据〔2025〕18 号）。

〔67〕戴昕：《作为法律技术的安全港规则：原理与前景》，载《法学家》2023 年第 2 期，第 37 页。

〔68〕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 98 页。

据并不会减损数据的聚合价值，而保护人们差异化的隐私偏好反而可以尊重信息主体的尊严性隐私并因此提升整体福利水平。因此，同意规则完全可以在整体形式化的前提下将规范重心转移至保护实质不同意。

第一，可以将同意规则建构为“普遍默示的形式同意+具体明确的实质不同意”。《个人信息保护法》第27条的规则体现了此类规范思路：已公开个人信息的处理可以无须获得个人同意，但是当个人明确提出拒绝之后，不得处理已公开个人信息。司法实践采取了类似思路，北京互联网法院作出判决认定转载公开的招录信息并不构成侵权，但当信息主体提出删除请求后，保留转载内容将构成侵权。^{〔69〕}“默示同意+明示拒绝”的思路可以拓展至更一般化的信息流动场景。以公共场合拍摄为例，自媒体的迅速发展导致公共场所的拍摄成为普遍需求，但若要求拍摄者逐一征求被拍摄者的同意又不可行，因此可以将该场景中的默认规范设置为“默示的形式同意”，将被拍摄者表达拒绝拍摄或要求视频打码的行为理解为“实质不同意”。比如在“女孩被绑树教育”一案中，未成年女孩的监护人已经明确拒绝路人拍摄，拍摄者仍然持续拍摄并将视频内容发布至互联网，其行为被法院判定为侵权。^{〔70〕}

第二，可以将同意规则建构为“个人同意不与网络基础服务挂钩”。大量法学论证已经说明提供互联网信息服务的平台具有公共性，诸多网络服务已经成为人们生活中不可缺失的基础服务。因此，若信息处理者将网络基础服务与个人同意挂钩，个人没有任何选择空间；互联网的各类信息处理规则也就成为人们必须接受的规则。法律必须创造出信息主体作出实质不同意的决策空间。《个人信息保护法》第16条发挥了“维护不同意决策空间”的制度功能，其通过捆绑禁令的方式将个人同意与网络服务松绑。^{〔71〕}对个性化推荐的规制也体现了相似的思路，由于互联网平台经济依赖基于个人信息处理的精准匹配，因此捆绑禁令并不足以支撑实质不同意的决策空间，故《个人信息保护法》第24条第2款支持个人拒绝个性化推荐。

法律在创设不同意决策空间时需要顾及同意规则的分配后果。其一，对部分隐私偏好群体的保护可能会减损整体福利，比如信息处理者需要专门设计缺少个人信息时的交互页面。就此而言，法律规制不可能完全精准，部分隐私偏好将无法被满足，信息主体无法作出不同意决策。其二，若法律尊重与保护个人的拒绝权，个人信息处理者是否也有一定程度上的拒绝个人接入权。这或许是《个人信息保护法》第16条后半句的含义，当个人信息处理者提供的产品或者服务需要个人信息但个人拒绝提供的，企业有权拒绝接入。其三，对不同意决策的保障可能会产生经济后果。

〔69〕《北京互联网法院涉个人信息及数据典型案例》，载北京互联网法院2024年10月31日，https://m.thepaper.cn/baijiahao_29205833。

〔70〕《李某某诉魏某、某网络技术有限公司网络侵权责任纠纷——公共场所未成年隐私权的认定与保护》，人民法院案例库入库编号，2023-14-2-369-001。类似案例还有，《平台上传食客就餐视频被判侵犯肖像权 汉阳法院：删除视频并赔偿道歉》，载《湖北日报》2024年12月11日，第9版。

〔71〕付举乾：《“信息换给付”下捆绑禁令的内在体系与规范构造——对〈个人信息保护法〉第16条的解读》，载《交大法学》2024年第6期，第126页。

有研究预测，若严格执行欧盟的数据隐私法，大型、通用平台将会获得竞争优势，而小型、专业化的公司运营成本将会上升⁽⁷²⁾，这是因为人们更有可能对小型、专业化公司中的个人信息处理作出实质不同意决策。

第三，可以将同意规则建构为“个人的不同意若直接指向具体的信息用途与流向，个人可以作出精准的不同意决策”。在一些场景中，信息主体未必期待禁止信息流动，而是期待对信息流动的后果有所控制；当信息流动的后果无法控制时，信息主体才会倾向于禁止信息流动。比如，在携程大数据杀熟案中，原告胡女士虽以同意规则作为请求权基础，但其实质请求却是“拒绝大数据杀熟”⁽⁷³⁾；而朱某诉百度案中，朱某未必反对百度网站收集 Cookie，但若百度网站收集、使用 Cookie 无法做到对信息主体尊严性隐私的保护，信息主体就会选择限制信息流动。就此而言，同意规则在规范设置上应当尽可能为信息主体表达具体诉求预留规则空间。《个人信息保护法》体现了此种思路，第 24 条第 2 款为个人拒绝自动化决策提供了规范依据；第 26 条限制了公共场所监控信息的用途。对用途与信息流动后的接触（access）状态的限制更是公共空间隐私处理的一般规范，法律不太可能限制公共空间中的信息流动，但法律可以限制公共空间中的信息接触，即采取“看破不说破”“可见不可看”⁽⁷⁴⁾的规则策略。不过，信息主体对信息流动后果的限制还取决于制度目标，比如公开裁判文书中的个人信息。⁽⁷⁵⁾

（三）同意规则的事前事后面向

对同意规则的规范重构还需要考虑规则的事前面向与事后面向。事前面向是指需要考虑面向未来的规则设计、个案裁判可能对未来发生的影响，属于分配正义范畴，比如是否将某种信息流动方式设置为一般化的规范；事后面向指的是在单个案件中事后补救，属于校正正义范畴，比如支持特定信息主体提出的实质不同意请求。⁽⁷⁶⁾

基于上文对“实质不同意”的论述，同意规则在法律实践面临的争议场景中可以采取事后面向。理由如下：其一，对于特定信息主体的不同意请求，同意规则通过对实质不同意的保护可以实现对其尊严与自主的保护；其二，若经济社会对同意规则的具体实施方式已经有了共识，那么可能产生的争议多来自信息流动带来的新场景、新用途，这部分信息流动对社会福利仅产生边际上的影响，对争议的解决应以事后个案化处理为主；其三，信息产业的发展有赖于信息关联性的

〔72〕 James Campbell, Avi Coldfarb, Catherine Tucker, *Privacy Regulation and Market Structure*, 24 *Journal of Economics & Management Strategy* 47, 47 (2015).

〔73〕 潘永建、朱晓阳、王雪莹、周鑫：《“大数据杀熟第一案”代理随笔——简评胡某诉携程案二审判决》，载通力律师事务所 2022 年 1 月，https://www.llnkslaw.com/uploadfile/publication/9_1643105020.pdf。

〔74〕 岳林：《论公共空间的隐私》，载《思想战线》2020 年第 3 期，第 144 页。

〔75〕 张鼎：《裁判文书公开的声誉影响及其规范控制》，载《西南政法大学学报》2024 年第 1 期，第 147 页。

〔76〕 [美] 沃德·法恩斯沃思：《高手：解决法律难题的 31 种思维技巧》，丁芝华译，法律出版社 2016 年版，第 8 页。

发现,尤其是未来社会治理、经济发展需要拓展个人信息的关联性与应用场景⁽⁷⁷⁾,因此要求信息处理者事前就可能产生的新拓展、技术黑箱中的信息处理方式征求个人同意并不现实⁽⁷⁸⁾。除了经济效率、分配正义的考量外,技术的发展正使告知—同意的必要性下降,隐私计算技术使得信息处理者可以在不触及原始数据、原始数据不出域的情况下实现信息处理,法律重心应当转变为推动信息的非明文流动。⁽⁷⁹⁾

同意规则事前面向的采取需要在社会共识的基础上作出。有学者已经指出,在中国通过个案的方式改进同意规则并不具备可行性⁽⁸⁰⁾,但这并非因为司法案例难以上升为规则,而是因为以个案中具体的信息流动分配秩序上升至整个社会的分配秩序有待检验。何况,社会人群中本就有着分化严重的隐私偏好,规则形成所需的社会共识难以达成。在一些场景中,社会可能会形成共识,比如生成式人工智能(AIGC)输出真实个人信息的问题,根据AIGC的技术原理,其中的信息流动可能是输出的个人信息为互联网上可获取的真实信息,人工智能在用户提问引导下输出整合后的个人真实信息。⁽⁸¹⁾由于共识性较高,人工智能开发者很快就通过技术方案优化了输出内容。此案例同样说明,同意规则的事前面向不必局限于司法个案,而是可以表现为监管细则、行业自律,借助同意规则的传声筒功能实现规制目标。

上文对同意规则的规范重构表明,同意规则的形式化并不意味着疏忽与减弱对信息主体权益的保护;反而,重构后的形式化同意规则可以实现个人信息保护与利用之间的平衡。

四、结语

随着信息产业、数字经济的进一步发展,无处不在的信息收集、快捷的信息传输、复杂的信息处理与分析将会成为未来经济发展、社会治理的基础,而这一切需要法律制定合适的信息流动规范。已有的法律制度,包括但不限于成文的《个人信息保护法》将个人的同意作为信息流动的基础;此种制度设置本身并不会限制信息流动甚至会有利于形成既保护信息主体又能促进信息流动的均衡。但若法律理论将个人的同意理解为实质同意,即通常所描绘的“有效告知、充分知情、实质同意”,那么当前的个人信息处理实践无疑已经表明,信息主体不太会也不太可能作出实质同意;冗长的告知同意文本可能成为增加信息主体认知负担、干扰用户网络体验的障碍,甚至成为

(77) Salomé Viljoen, *A Relational Theory of Data Governance*, 131 *The Yale Law Journal* 573, 609 (2021). 有关可能的技术应用场景,参见《图计算如何成为下一代数据底座?》,载《21世纪经济报道》2022年9月2日,第8版;史中、浅黑科技:《支付宝有多狠?当年为抓骗子搞出“图计算”,现在竟用它预测未来》,载微信公众号“浅黑科技”2024年1月5日, <https://mp.weixin.qq.com/s/i3iVahvHigK2Q9gFVZDlmQ>。

(78) 黄镔:《生成式AI对个人信息保护的挑战与风险规制》,载《现代法学》2024年第4期,第103页。

(79) 张晔:《隐私计算:让数据“可用不可见”》,载《科技日报》2023年4月10日,第6版。

(80) 衣俊霖:《论个人信息保护中知情同意的边界——以规则与原则的区分为切入点》,载《东方法学》2022年第3期,第59页。

(81) 《豆包AI能否搜出个人隐私?平台回应:基于公开信息,已优化保护》,载腾讯开放平台2024年12月11日, https://page.om.qq.com/page/OmAnlO9HLS6UuIR7P5zrEV_Q0。

法律陷阱。就此，笔者提出，法律理论对同意规则的理论建构应当抛弃实质同意这一不现实的目标，转而在形式化同意规则上重构同意规则，将同意规则作为个人信息处理的程序性要求，将其制度重心转移至尊重与保护信息主体在信息互动中作出的“实质不同意”决策，顾及不同群体的隐私偏好。

将同意规则进行形式化改造所需要的规则变动成本极低。部分学术理论认为应当弱化甚至废止同意规则，这类方案未能注意到同意规则不仅是《个人信息保护法》的成文规则，更是诸如网络安全法、数据安全法、消费者权益保护法以及诸多部门规章的成文规则，直接废止的改造成本过于高昂，而弱化适用又没有具体方案。将同意规则形式化处理并不需要改造当前的法律规则，甚至也无须变动当前的执法、司法实践，因为形式化的同意规则仅是将客观的法律实践上升为法律理论。之于未来的经济发展与社会治理而言，形式化的同意规则同样有利于经济发展与数字治理措施的优化，因为信息的收集、处理与使用无须追求信息主体的实质同意，仅需要在最低限度上履行法律的程序性要求获得个人的形式同意。这并不意味着法律放弃对个人自主与尊严的保护，而是将监管重心转向更能影响信息主体福利、风险状况的信息处理行为，并不是只寄希望于同意规则。也就是说，与其追求实质同意，不如在形式化同意规则的基础上更实质性地关注信息主体的权益，一言以蔽之，无需实质同意。

Consent Without Substance: Formalized Consent Rules and Its Functions

ZHANG Ding

Abstract: Consent rules, as rules for personal information processing, are formalized in practice. Formalized consent rules have normative implications. Existing theories making the goals of consent rules as pursuing substantive personal consent to guarantee individual autonomy. However, due to cognitive state of data subjects, institutional structural constraints of decision-making, and relational attributes of information flow, the possibility for data subjects to give substantive consent is small. There is discrepancy between institutional goal and reality. Formalized consent rules derive unexpected functions, including serving as safe harbor for information processing activities, mouthpiece for information regulation, and cradle for nurturing digital trust. The functions and advantages of formalized consent rules indicate that there is no need to abolish consent rules. The transformation of consent rules requires abandoning substantive consent and re-understanding and reconstructing consent rules around formalized consent. Specific

normative suggestions include: transforming consent rules into a prerequisite procedure that information processing activities must undergo; shifting the regulatory focus of consent rules to protecting data subjects' substantive non-consent decisions; and distinguishing between the ex-ante and ex-post aspects of consent rules.

Keywords: Formalized Consent Rules; Personal Information Processing; Substantive Non-consent Decisions; Digital Trust

(责任编辑: 王乐兵 汪友年)