

DOI: 10.53104/fxsy.2026.02.04.003

数字服务场景下个人信息知情同意的形式化困境

赵腾¹

1. 河北大学, 河北 保定 071000

摘要: 知情同意是个人信息保护制度中的重要规则, 其目的在于使个人了解自身信息将被如何收集、使用, 并在此基础上作出自主选择。当前, 购物、社交、短视频、出行等数字服务普遍通过隐私政策、授权弹窗和服务协议取得用户同意, 但形式上的“同意”并不意味着用户真正理解并接受相应的信息处理活动。实践中, 隐私政策内容冗长、授权事项集中设置、必要信息与非必要信息混合、后续用途变化提示不足以及撤回同意困难等现象, 使知情同意逐渐成为进入数字服务之前的一项程序性操作。用户虽然完成点击, 却可能并未形成真实、明确的意思表示。本文以数字服务中的个人信息处理为主要场景, 在《个人信息保护法》现有规则基础上, 对知情同意形式化的主要表现及其形成原因进行分析。知情同意形式化既与服务提供者和用户之间的信息不对称有关, 也受到持续性数据处理、平台商业利用需求以及偏重形式合规等因素影响。对此, 应改进告知方式, 区分必要与非必要个人信息, 减少概括授权, 在个人信息处理目的和方式发生重要变化时强化再次确认, 同时降低撤回同意的操作成本, 使知情同意从一次性的形式确认转向贯穿个人信息处理过程的持续选择。

关键词: 数字服务; 个人信息保护; 知情同意; 形式化; 用户控制

The Formalization Dilemma of Informed Consent for Personal Information in Digital Services

ZHAO Teng¹

1. Hebei University, Baoding 071000, P. R. China

Correspondence to: ZHAO Teng

Abstract: Informed consent is an important rule in the protection of personal information. Its purpose is to enable individuals to understand how their personal information will be collected and used and to make autonomous choices on that basis. At present, digital services such as online shopping, social networking, short-video platforms, and mobility services commonly obtain users' consent through privacy policies, authorization pop-ups, and service agreements. However, formal "consent" does not necessarily mean that users truly understand and accept the relevant personal information processing activities. In practice, lengthy privacy policies, bundled authorization settings, the mixing of necessary and non-necessary personal information, insufficient notice of changes in data use, and difficulties in withdrawing consent have gradually reduced informed consent to a procedural step before users can access digital services. Although users may click to agree, their consent may not always reflect a genuine and explicit expression of will. Focusing on personal information processing in digital services, this paper examines the main forms and causes of the formalization of informed consent within the existing framework of the Personal Information Protection Law. It argues that this

引用格式: 赵腾. 数字服务场景下个人信息知情同意的形式化困境[J]. 法学视野, 2026, 2(3): 16-25.

formalization is related not only to information asymmetry between service providers and users, but also to continuous data processing, commercial incentives for broader data use, and compliance practices that place excessive emphasis on formal procedures. To address these problems, service providers should improve the way information is disclosed, distinguish between necessary and non-necessary personal information, reduce broad and bundled authorization, require renewed confirmation when the purpose or method of personal information processing changes significantly, and lower the practical cost of withdrawing consent. In this way, informed consent can move from a one-time formal confirmation toward a continuous mechanism of user choice throughout the process of personal information processing.

Key words: digital services; personal information protection; informed consent; formalization; user control

引言

各类数字服务在提供购物、社交、出行、娱乐、支付等功能时，往往需要处理用户的手机号、位置、交易记录、浏览记录以及设备信息等个人信息。一部分信息是完成服务所必需的，还有一部分信息主要用于个性化推荐、商业营销、用户画像或者产品改进。在多数数字服务中，平台经营者既是服务提供者，也是个人信息处理活动的重要组织者。个人很难完全脱离个人信息处理活动使用这些服务，个人信息的收集和利用也因此成为数字生活中的常见现象。

个人信息的合理利用能够提高服务效率，也可能对个人权益产生影响。特别是在服务提供者掌握大量用户信息后，普通用户并不容易判断具体收集了哪些信息，这些信息将用于什么目的，是否会提供给其他主体，又会保存多长时间。任海波、安雪文在研究生成式人工智能中的个人信息保护问题时，也注意到信息收集、算法分析及内容输出过程中可能出现过度收集、违规处理和过程不透明等风险^[1]。这些问题虽然产生于不同技术环境，但都反映出个人与信息处理者之间存在明显的信息掌握差距。

在这一背景下，知情同意承担了连接个人信息利用与个人自主决定的重要作用。《个人信息保护法》第14条规定，基于个人同意处理个人信息的，同意应当由个人在充分知情的前提下自愿、明确作出；个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，还应

重新取得同意。第15条规定个人有权撤回同意，个人信息处理者应当提供便捷的撤回方式。第16条对“不同意就不能使用”的做法作出限制，第17条则要求处理者以显著方式、清晰易懂的语言履行告知义务。由此可以看出，法律所要求的并不是简单获得一个“同意”按钮的点击结果，而是要求同意建立在真实知情和自主选择之上。

现实中的数字服务却容易把同意转化为进入服务前必须完成的一个操作步骤。用户点击“同意并继续”后，服务提供者即认为已经完成告知和授权程序。此时同意的法律形式已经具备，用户的实际选择却未必真正形成。罗世杰在研究金融数据共享时指出，一次性授权和静态分类容易导致知情同意趋于静态化和形式化，并提出持续披露、授权调整、再次确认和撤回控制等改进思路^[2]。这种判断同样能够用于观察一般数字服务中的个人信息处理活动。

本文所讨论的“知情同意形式化”，主要是指个人信息处理者表面上履行了告知并取得用户同意，但由于告知、选择或者撤回机制本身存在不足，用户实际上难以形成充分知情、自愿和明确的意思表示。本文不讨论个人信息保护制度的全部问题，也不涉及复杂的算法技术，而是集中分析数字服务中知情同意为何容易失去实质作用，以及如何在现有法律框架下进行改进。

1 数字服务中个人信息知情同意的基本要求

1.1 知情与同意不能相互分离

知情同意包含“知情”和“同意”两个相互联系的部分。没有充分知情，同意缺乏作出判断的基础；只有告知而没有选择，也不能形成真正有效的同意。服务提供者向用户展示隐私政策，只能说明告知程序已经开始，并不能直接推定用户已经理解其中的内容。

《个人信息保护法》第17条要求处理者在处理个人信息之前，告知处理者名称或者姓名、联系方式、处理目的、处理方式、个人信息种类、保存期限以及个人行使权利的方式和程序。法律还特别要求告知采用显著方式和清晰易懂的语言。这意味着判断个人信息处理者是否履行告知义务，不能只看是否提供了一份隐私政策，还需要观察关键信息是否真正能够被普通用户发现和理解。

同意则强调用户作出选择的自主性。根据《个人信息保护法》第14条，同意应当在充分知情的前提下自愿、明确作出。这里的“自愿”意味着服务提供者不能通过不合理限制迫使用户接受与基本服务没有直接关系的信息处理。“明确”则要求用户能够知道自己究竟同意什么，而不能把大量不同目的、不同性质的信息处理行为全部放入一个笼统授权之中。

知情与同意实际上构成一个连续过程。用户需要先知道服务提供者准备处理哪些个人信息，再判断这些处理行为是否可以接受。如果信息处理目的、方式或者信息种类后来发生变化，原有判断基础已经改变，过去作出的同意也不能当然覆盖新的处理活动。

1.2 同意并不是处理个人信息的唯一依据

讨论知情同意时，还应避免将所有个人信息处理行为都理解为必须取得同意。《个人信息保护法》第13条列举了处理个人信息的合法基础，取得个人同意只是其中一种。订立和履行合同所必需、履行法定职责或者法定义务所必需等情况下，也可以依法处理个人信息。这一点对于数字服务中的个人信息处理十分重要。如果不区分不同处理依据，很容易形成“所有信息都放进隐私政策，再由用户一次性同意”的做法。购物服务完成商品配送可能确实需要收货地址和联系电话，但利用购买记录开展额

外商业营销，则不能简单认为与履行购物合同具有同样的必要性。

付新华关于个人信息处理合法性基础的研究指出，个人信息处理的合法性判断不能只围绕个人同意展开，还需要考虑处理目的、处理必要性以及不同主体之间的利益关系^[3]。这说明，同意本身并不是服务提供者无限扩大个人信息处理范围的工具。用户曾经点击同意，也不意味着以后所有处理活动都自然获得合法依据。区分不同处理依据还有一个现实意义，即能够减少数字服务对同意机制的过度依赖。真正属于提供基本服务所必需的信息，可以依据法律规定处理；超出必要范围的信息利用，则应重新判断是否需要个人作出选择。这样反而可以使知情同意集中于真正需要用户自主判断的事项。

1.3 知情同意的核心是保持个人的实际选择能力

从个人角度看，知情同意最现实的作用，是让用户能够对个人信息处理作出决定。冯明昱在讨论健身数据开发利用时指出，连续服务中容易出现用户控制权不足，概括授权、整体退出和形式化的权利行使安排不能支持用户对特定利用事项作出有效选择^[4]。虽然该研究针对健身数据，但其中反映的问题并不限于这一具体场景。

购物、视频、社交、地图等数字服务同样存在持续处理个人信息的情况。用户注册时的一次同意可能发生在数月甚至数年前，而服务内容之后还可能增加新的功能、改变推荐方式或者增加合作主体。如果仍然完全依赖最初的授权，用户很难对后续处理活动保持实际控制。

判断知情同意是否有效，因而不能只问“用户有没有点同意”，还应进一步考察用户是否看得到重要信息，是否能够拒绝非必要事项，处理方式发生变化后是否能够重新选择，以及已经同意之后能否方便撤回。换言之，知情同意真正需要保护的不是一个点击动作，而是个人对信息处理行为持续作出决定的能力。只有用户具备现实的选择空间，形式上的同意才具有实际意义。

2 数字服务中知情同意形式化的主要表现

2.1 告知内容完整但用户难以真正阅读

隐私政策是数字服务提供者履行告知义务的主要方式。它能够集中说明个人信息处理的基本情况,也方便服务提供者留存合规记录。不过,隐私政策通常包含大量法律术语、技术说明、第三方服务情况和权利行使规则。如果只追求把所有事项完整写进文本,隐私政策很容易变得越来越长。这种情况下会出现一个明显的问题:从形式上看,告知的信息十分充分;从用户实际阅读情况看,获取重要信息反而更加困难。普通用户进入数字服务通常是为了购物、观看视频、使用导航或者与他人交流,很少会在正式使用之前逐条阅读篇幅较长的隐私政策。把大量事项放进同一个文本,并不必然意味着用户已经充分知情。问题的关键并不是要求隐私政策缩短到极少内容,而是应当区分信息的重要程度。例如,收集手机号码用于注册账号和调用通讯录用于寻找好友,对用户产生的影响并不相同;将个人信息提供给新的第三方,也不同于在服务提供者内部完成基本服务。对这些影响较大的事项,仅在长篇隐私政策中出现一次,告知效果十分有限。《个人信息保护法》第17条要求使用显著方式和清晰易懂的语言,也说明法律关注的并非纯粹的文本完整性。告知应当使普通用户较为直接地理解重要事项,而不是把全部理解责任交给用户。

2.2 多个处理目的被集中为一次概括授权

知情同意形式化的另一种常见表现,是把多个个人信息处理目的放进一次授权中。用户只面对“同意”或者“不同意”两个选项,无法分别决定是否接受不同的信息利用方式。

服务提供者为了实现基本功能收集必要信息具有现实基础。例如,网上购物需要一定的联系方式和收货信息,地图导航需要位置信息。《常见类型移动互联网应用程序必要个人信息范围规定》按照不同App基本功能划定必要个人信息范围,并明确不能因为用户拒绝提供非必要个人信息而拒绝其使用基本功能。必要

信息与附加功能所需要的信息并不处于完全相同的位置。

概括授权却容易模糊这种区别。用户可能只是想完成一次购物,却同时被要求接受个性化推荐、营销信息推送或者其他用途的数据利用。多个目的被包装在一个“同意并继续”按钮之下以后,用户就很难针对其中某一个事项单独表达拒绝。冯明昱指出,概括授权不足以支撑用户对特定数据利用事项作出有效选择^[4]。这正是形式化同意的重要问题。授权范围越宽,用户实际知道自己同意什么就越困难。形式上的授权越集中,用户实质上的选择反而可能越弱。

2.3 拒绝同意与停止使用服务被过度绑定

数字服务提供者与普通用户之间并不是完全对等的关系。对于使用频率较高的购物、社交、支付或者出行服务而言,拒绝相关协议有时意味着用户无法继续使用已经较为熟悉的服务。这会使所谓的“同意”带有较强的被动色彩。

《个人信息保护法》第16条已经明确,个人信息处理者不得以个人不同意处理个人信息或者撤回同意为由拒绝提供产品或者服务,但个人信息属于提供产品或者服务所必需的除外。相关App必要个人信息规则也要求,不得因为用户拒绝提供非必要个人信息而拒绝其使用基本功能。

现实中的问题更多发生在“必要”与“非必要”的边界上。如果服务提供者把个性化推荐、商业推广所需要的信息与基础服务混合起来,用户就容易面对“全部接受”或者“放弃服务”的选择。此时虽然页面上存在同意按钮,但这种选择距离真正自愿仍有差距。

用户的同意不能成为扩大信息处理范围的当然理由。特别是在平台经营者拥有较强服务控制能力的情况下,判断同意是否自愿,更应关注用户拒绝某项非必要处理后是否还能正常使用基本服务。

2.4 后续用途变化仍依赖最初的一次同意

数字服务中的个人信息处理往往具有持续性。用户注册账号只是信息关系的开始,后续

还会不断产生搜索记录、购买记录、位置信息、观看记录和互动记录等数据。服务模式也可能发生改变,个人信息最初用于完成某项基本功能,后来又可能被用于内容推荐、商业营销、风险分析或者新的业务场景。

罗世杰指出,高频流转和用途扩张使以一次性授权为基础的知情同意模式面临制度失配,个人的知情同意权容易因此趋于静态化和形式化^[2]。这一判断对一般数字服务具有较强的解释力。

如果用户注册时已经勾选相关协议,服务提供者后来便把最初的同意理解为长期授权,实际上忽略了同意所依赖的具体处理目的。《个人信息保护法》第14条已经明确,处理目的、处理方式或者个人信息种类发生变更,应当重新取得个人同意。重新同意并不是重复进行一次没有意义的操作,而是因为用户原有判断所依据的条件已经发生改变。

刘乐乐在研究生成式人工智能背景下个人信息民法保护时指出,个人信息利用已经从传统的静态处理转向训练、推断、生成和反馈优化相互交织的动态处理,传统知情同意、目的限制、最小必要和公开透明等规则面临新的适用压力,并提出分级同意和动态同意等改进方式^[5]。普通数字服务虽然不一定都涉及生成式人工智能,但持续处理和用途变化的问题已经较为普遍。仅靠用户刚进入服务时的一次授权,很难完整覆盖后续不断变化的信息处理活动。

2.5 撤回同意存在入口隐蔽和操作复杂问题

知情同意并不意味着用户一旦接受便不能改变决定。《个人信息保护法》第15条明确规定个人有权撤回同意,并要求个人信息处理者提供便捷的撤回方式。

从权利结构看,撤回同意与作出同意同样重要。如果同意只需要点击一次按钮,而撤回却需要进入多个页面、查找隐蔽设置、联系客服甚至注销账号,用户作出选择和改变选择的成本明显不对等。

形式上的撤回入口也不当然意味着撤回权已经得到保障。数字服务中可能同时存在“关闭个性化推荐”“管理权限”“隐私设置”等不同入口,普通用户不一定清楚哪项操作真正

对应撤回同意。有些权限可以通过手机系统关闭,但关闭设备权限也不一定意味着此前已经收集的信息会停止被使用。

罗世杰提出的授权调整、撤回控制和持续维护思路^[2],说明知情同意不应只关注授权入口,还应关注同意之后的控制过程。如果退出明显比进入困难,用户的控制权仍然可能停留在形式上。

3 知情同意形式化的形成原因

3.1 服务提供者与用户之间存在明显的信息不对称

服务提供者决定个人信息处理的技术方式、业务目的和具体流程,对信息流向具有较强掌握能力。普通用户则主要通过隐私政策和提示信息了解处理情况,这种信息来源本身带有较强的单向性。

用户还缺乏判断某些信息处理后果所需要的专业知识。例如,单独来看某一项浏览记录可能并不敏感,但与消费、位置、设备等信息结合后,可能形成更加完整的用户特征。王翰文指出,敏感个人信息保护需要结合具体场景,进一步考虑信息类型、利用方式和可能产生的风险^[6]。这类判断对于普通用户而言并不容易完成。如果服务提供者只是把复杂信息原样交给用户,再要求用户自行承担阅读和判断责任,知情同意很容易退化为形式程序。减少这种差距不能单纯依赖用户提高个人信息保护意识,更需要信息处理者主动改善告知方式和授权结构。服务提供者掌握的信息越多、处理方式越复杂,越不能简单把“已经提供隐私政策”作为完成告知义务的全部依据。

3.2 服务提供者具有扩大个人信息利用范围的现实需求

个人信息不仅能够用于完成当前服务,还可以用于用户分析、内容推荐和商业营销。对数字平台经营者而言,能够合法获得的信息范围越广,后续利用空间通常也越大。这形成了扩大信息利用范围的现实动力。

概括授权能够减少多次征求用户同意的操作成本。一份隐私政策、一次集中授权,显然比

针对不同目的分别设置选择更加便利。但服务提供者的便利不能完全替代用户的自主选择。

阚玉茜在算法价格歧视研究中指出,平台利用用户消费习惯、支付意愿、行为特征等信息开展差异化定价时,可能同时影响消费者的知情权、自主选择权、公平交易权和个人信息权益,而实践中还存在知情同意流于形式的问题^[7]。虽然算法价格歧视只是个人信息商业利用的一种具体场景,但它能够反映数据商业价值与用户个人信息权益之间的现实张力。

知情同意形式化因而不只是隐私政策太长或者按钮设置不合理的问题。其背后还涉及服务提供者降低运营成本、提高数据利用效率的现实需求。如果对这种扩张动力缺乏合理约束,用户的一次同意就很容易被解释为更广泛、更长期的信息使用许可。

3.3 个人信息处理已由单次收集转向持续处理

传统场景下,个人信息处理可能只是填写一张表格,收集目的相对容易确定。数字服务中的信息处理则常常伴随整个服务过程。用户每一次搜索、浏览、购买和互动,都可能产生新的信息。

持续处理使一次性同意的局限更加明显。用户刚注册时无法准确预见未来服务提供者将增加哪些功能,也难以判断相关信息是否会产生新的用途。刘乐乐提出,面对动态个人信息处理活动,应通过分级同意、动态同意、目的兼容性判断以及关键信息说明等方式提升传统规则的适应能力^[5]。

赵伟在研究具身智能风险时,也将传统知情同意机制的结构性失效作为重要问题,并提出建立分级动态同意机制^[8]。不同研究场景虽然有所区别,但共同反映出一个问题:面对持续变化的信息处理活动,仅依靠最开始的一次同意,已经越来越难以维持用户对个人信息的实际控制。

过去的一次授权原本对应较为确定的信息处理活动,现在却可能被用于覆盖持续产生、不断变化的信息利用行为。同意本身没有变化,但信息处理活动已经发生改变,两者之间自然容易出现脱节。

3.4 合规实践容易偏重“留下同意记录”

在发生个人信息争议时,服务提供者往往需要证明自己已经履行个人信息保护义务。因此,是否存在用户勾选记录、隐私政策是否展示、系统是否保存授权时间,都具有实际意义。

这种证明需求本身具有合理性,但如果合规工作过分集中于证明“用户点过同意”,就可能忽略同意形成的过程是否真实。知情同意容易被理解为一套页面、按钮和系统记录,而不是用户参与个人信息处理决定的权利机制。

相关研究指出,经营者不当处理消费者个人信息容易引发民事纠纷,而信息主体在取证和损害救济方面仍存在现实困难^[9]。在双方掌握证据明显不对等的情况下,如果只依据经营者保存的勾选记录判断个人是否有效同意,可能进一步强化信息处理者在争议中的优势。

知情同意的判断应当从“有没有同意记录”逐渐转向“同意是怎样形成的”。告知是否显著、语言是否容易理解、拒绝是否影响基础服务、不同目的能否分别选择,都应成为判断的重要因素。

4 知情同意形式化对个人信息权益的影响

知情同意形式化最直接的后果,是削弱个人对自身信息处理活动的实际控制。用户虽然在法律形式上作出了同意,但可能并不知道信息被收集的具体范围,也不清楚同意之后会发生何种利用。

当用户缺少对处理目的和处理方式的真实认识时,其所谓自主决定实际上已经受到限制。个人信息保护中的“同意”原本应体现个人对信息利用活动的判断,但形式化同意却把这种判断简化成进入服务之前的点击步骤。久而久之,用户容易形成“不点击就无法继续”的习惯,对隐私政策和授权提示不再认真关注。

这一问题在敏感个人信息处理中更加突出。生物识别、医疗健康、金融账户、特定身份等信息一旦被不当处理,可能给个人带来更高风险。高完成、王帅淙指出,个人生物识别信息

既属于敏感个人信息，又可能涉及隐私和人格利益，其保护不能仅停留在一般的信息处理规则层面^[10]。对这类信息，如果仍然采用一般性的概括授权，形式同意造成的风险会更加明显。

形式化同意还可能扩大个人信息利用范围。信息处理者获得较宽泛授权后，用户很难判断某项后续处理是否真的包含在过去同意的范围内。时间越长，处理方式变化越多，最初同意与当前处理活动之间的联系就越弱。即使服务提供者仍能够展示最初的同意记录，也不意味着当前处理行为仍然具有充分的授权基础。

自动化决策场景进一步说明了这一问题。

《个人信息保护法》第24条赋予个人在特定自动化决策中的说明请求和拒绝相关权利。徐一丹认为，要求说明权和自动化决策拒绝权能够矫正信息不对称，并增强个人对自动化决策过程和控制的控制^[11]。如果个人在信息收集阶段就缺乏真实选择，后续对自动化处理个人信息的控制难度还会进一步增加。

知情同意形式化最终影响的并不是一项孤立的程序权利，而是个人对自身信息流向和用途的整体控制能力。如果最初的授权基础已经空洞化，后续查阅、更正、删除、限制处理等权利的实际作用也可能受到影响。

5 数字服务中知情同意机制的完善

5.1 从形式完整的告知转向关键信息的有效传达

解决知情同意形式化问题，并不是简单减少告知内容。个人信息处理事项较为复杂，完整的隐私政策仍然有必要保留。更适合的方式，是在完整告知的基础上建立分层提示机制。

服务提供者可以在完整隐私政策之外，把直接影响用户选择的重要事项单独提示。例如，是否调用通讯录、是否持续获取位置、是否向第三方提供信息、是否利用信息进行个性化推荐等，都可以通过较短的提示向用户说明。

一般性的信息处理事项可以放在完整政策中供用户查询，重要事项则应在实际发生前进行明确提示。这样既能够保留法律文本的完整性，也能降低用户获取关键信息的成本。在文

字表达上，也应适当减少过度专业化的内容。法律要求“清晰易懂”并不是要求放弃准确性，而是要求法律、技术和商业语言经过适当转换，使普通用户能够理解自己的信息为什么被收集、将如何使用以及自己能否拒绝。

告知制度真正需要实现的是“让用户知道”，而不是“让信息处理者留下已经告知的证明”。只有用户能够较容易发现和理解重要信息，后续作出的同意才具有较好的实质基础。

5.2 明确区分基础服务必要信息与附加用途信息

取得用户同意之前，应当先区分完成基础服务所必需的信息与用于附加功能的信息。对前者，可以依据合同履行需要或者其他合法基础依法处理；对没有直接必要性的额外用途，则不能通过捆绑方式迫使用户接受。

《常见类型移动互联网应用程序必要个人信息范围规定》已经为不同类型App划定必要信息范围，并明确不得因用户拒绝提供非必要信息而拒绝其使用基本功能。这一思路可以直接用于限制知情同意形式化。例如，购物服务需要收货地址完成配送，并不意味着用户必须同时接受营销画像；视频服务提供普通内容播放，也不意味着所有用户都必须开放与基础播放无关的设备权限。服务提供者应当把这些不同用途适当拆分，使用户能够进行有针对性的选择。这种做法并不意味着每处理一次信息都要弹出窗口。过于频繁的授权同样会造成用户疲劳。较为合理的方式是按照功能和风险划分授权事项，只对具有实质区别的信息处理目的提供独立选择。

5.3 减少概括授权并强化重要事项的单独确认

对于处理敏感个人信息、向其他处理者提供个人信息、公开个人信息等风险较高的行为，《个人信息保护法》已经规定了单独同意等更加严格的要求。这类规则背后的基本逻辑，就是不能让重要处理事项被一般授权所淹没。

王翰文认为，敏感个人信息保护需要结合具体场景、信息用途和风险进行分类判断^[6]。这种场景化思路也可以用于数字服务中的授权设计。并不是所有个人信息都必须采用完全相同的同意强度，风险越高、偏离基础服务越明显，

越有必要进行单独提示和确认。

单独同意也不能只是增加一个新的按钮。如果提示内容与普通授权完全相同,或者用户不点击就无法继续任何服务,仍然可能只是增加了新的形式。真正有意义的单独同意,应让用户知道这一处理行为与一般处理有什么区别,以及拒绝后究竟会产生什么影响。实践中可以把授权事项按照“基础服务”“附加功能”“敏感信息处理”“对外提供”等类型适当区分。这样既不会使用户面对过多零散的选择,也能防止不同风险程度的信息处理被放进同一授权范围。

5.4 建立与用途变化相联系的再次同意机制

数字服务提供者不宜把用户注册时的同意视为长期不变的授权。个人信息处理目的、处理方式和个人信息种类发生变化时,应按照《个人信息保护法》第14条重新取得同意。如果只是进行不影响用户权益的一般技术调整,没有必要反复要求用户点击确认;但如果个人信息从完成基础服务转向商业推广,增加新的第三方接收主体,或者明显扩大敏感个人信息的处理范围,原有同意的基础已经发生变化,就有必要重新提示用户。罗世杰提出将知情同意从共享前的一次性授权转向全过程持续维护,并建立再次确认、授权调整和撤回控制等机制^[2]。这一思路可以避免两个极端:既不是每次处理都要求用户重新授权,也不是一次授权永久有效。

所谓“动态同意”并不依赖复杂的技术机制,其核心在于根据个人信息处理变化提供相应的重新选择机会。其基本规则可以较为简单:信息处理活动没有发生实质变化时,不反复打扰用户;处理目的、方式或者风险发生重要变化时,再重新提示并给予选择。

刘乐乐关于分级同意和动态同意的研究也说明,面对持续变化的数据处理方式,应把用户的选择机会与实际风险变化联系起来^[5]。对一般数字服务而言,这种做法比单纯增加更多隐私政策条款更具有现实可操作性。

5.5 使撤回同意与作出同意保持基本对等

用户能够方便撤回同意,是解决知情同意形式化问题的重要环节。服务提供者设置同意

入口时,也应同时考虑用户以后如何改变自己的决定。

比较合理的方式,是在隐私设置或者账号设置中建立统一的个人信息管理入口。用户可以直接查看主要授权状态,并关闭非必要的信息处理事项。服务提供者不宜要求用户为了撤回某项附加授权而注销整个账号,也不宜设置明显多于授权步骤的退出程序。

撤回后的法律效果也需要向用户说明。例如,撤回定位授权可能影响导航功能,但不应当当然影响与定位无关的服务;撤回个性化推荐授权后,可以改为提供非个性化内容,而不是直接停止全部服务。

冯明显提出,应当使用户能够在保留基础服务的情况下限制非必要的数据利用^[4]。这一思路能够较好处理数字服务正常运行与个人选择之间的关系。撤回同意并不意味着阻止服务提供者正常经营,而是要求不同信息用途与相应服务功能之间保持合理联系。只有当作出同意和撤回同意的难度大体相当,用户的选择权才具有连续性。否则,就容易形成“进入很容易,退出很困难”的局面,知情同意仍然会被固定在一次性的形式授权之中。

5.6 完善对知情同意实际效果的合规判断

监管和司法判断知情同意是否有效时,也应减少单纯依赖形式记录的做法。是否存在用户勾选记录当然可以作为证据,但还需要结合授权页面设计、告知内容、拒绝后果和撤回方式进行综合判断。

如果信息处理者能够证明已经提供清楚、独立的选择,并且用户拒绝非必要处理后仍然能够正常使用基础服务,则相应同意具有较强的真实性。相反,如果重要信息隐藏在长篇文本中,多个目的只能整体接受,用户一旦拒绝就不能使用基础服务,那么即使系统留下了“用户已同意”的记录,也应进一步判断这种同意是否符合充分知情、自愿和明确的法律要求。

陈彦铭通过对不同个人信息保护监管模式的比较指出,个人信息保护制度还需要通过规则细化、责任配置和监管机制提高实际运行效果^[12]。对于数字服务中的知情同意而言,真正

需要改善的也不是增加更多形式要求,而是使已有法律原则能够落实到具体的授权和服务过程之中。在这一过程中,可以逐步形成较为明确的判断因素,例如是否突出提示重要事项,是否区分不同处理目的,是否提供真实的拒绝机会,用户是否可以方便撤回,以及处理目的发生变化后是否再次取得同意。通过这些较为具体的标准,可以减少仅凭“用户已经勾选”判断处理行为合法性的倾向。

6 结语

知情同意并不是数字服务处理个人信息时需要完成的一项简单手续。其真正作用在于使个人能够了解信息处理活动,并保留接受、拒绝以及改变决定的可能。当前,各类数字服务已经普遍设置隐私政策和授权程序,但告知内容过长、概括授权、必要与非必要信息混合、一次授权长期使用以及撤回困难等问题,使部分

同意行为逐渐偏离其本来的制度目的。

《个人信息保护法》已经对充分知情、自愿明确同意、重新同意、撤回同意以及不得强制处理非必要个人信息作出了较为清楚的规定。现阶段更需要解决的,并不是重新构建一套复杂的知情同意理论,而是把这些要求落实到数字服务的具体运行过程中。服务提供者应当让重要信息更容易被看到,对不同处理目的作适当区分,在用途发生实质变化时重新给予用户选择,并提供与授权同样方便的撤回方式。

对知情同意的法律判断也不宜停留在“是否点击同意”这一层面。只有把告知是否有效、选择是否真实、拒绝是否可行以及撤回是否方便同时纳入考察,才能判断个人是否真正作出了自主意思表示。这样既可以减少个人信息保护中的形式主义问题,也不会否定数字服务合理处理个人信息的现实需求。

参考文献:

- [1]任海波,安雪文.生成式人工智能的应用对个人信息保护带来的挑战及应对策略[J].知识经济,2026(27):60-63.
- [2]罗世杰.论金融数据共享中信息主体知情同意权的动态保护[J].湖北经济学院学报.
- [3]付新华.正当利益作为大模型处理个人信息的合法性基础[J].政法论坛.
- [4]冯明显.用户控制权在健身数据开发利用中的实现机制[J].体育学研究.
- [5]刘乐乐.生成式人工智能背景下个人信息民法保护机制的完善[D].山东政法学院,2026.
- [6]王翰文.数智时代敏感个人信息分类规则面临的困境与对策[J].特区经济,2026(8):114-117.
- [7]阚玉茜.算法价格歧视侵害消费者权益的法律规制研究[D].山东政法学院,2026.
- [8]赵伟.从信息控制到人格守护:具身智能认知风险的法律规制进路[J].新媒体与社会.
- [9]ChenRuiyang.ACivilLawStudyontheProtectionofConsumers'PersonalInformation[J].JournalofSociologyandEducation,2026,2(6).
- [10]高完成,王帅淙.个人生物识别信息法律保护的困境及完善路径[J].征信,2026(8):11-20.
- [11]徐一丹.自动化决策中个人权利行使条件的法教义学分析[D].烟台大学,2026.
- [12]陈彦铭.双轨监管逻辑下的个人信息保护立法比较——以欧盟GDPR与韩国PIPA为研究中心[J].网络安全与数据治理.

版权声明

© 2026 作者版权所有。本文依据“知识共用署名 4.0 国际授权合约”（CC BY 4.0）以开放获取方式发布。该许可允许使用者在任何媒介中自由使用、复制、传播与改编文章（含商业用途），惟须明确署名原作者及出处，并注明所作修改（如有）。完整协议详见：<https://creativecommons.org/licenses/by/4.0/deed.zh-hans>

出版声明

所有出版物中的陈述、观点及资料仅代表作者及供稿者个人立场，与 Brilliance Publishing Limited 及/或编辑人员无关。Brilliance Publishing Limited 及/或编辑人员对因内容所提及的任何理念、方法、说明或产品所导致的人身或财产损害概不负责。