

网络平台隐私政策中知情同意原则的适用困境与破局思路

韩政原

上海大学, 上海

收稿日期: 2022年10月19日; 录用日期: 2022年11月1日; 发布日期: 2022年11月22日

摘要

知情同意原则作为个人信息保护的帝王原则, 其本身具有深厚的法理基础, 适用的困难不能作为动摇制度架构的理由。通过考察网络平台隐私政策中知情同意原则的实践困境, 分析知情同意原则适用困难的成因, 在此基础上提出通过明确和简化告知事项, 采用显著标识告知形式完善告知义务履行; 构建“理性人”标准的隐私政策, 建立动态同意机制和同意撤销机制增强同意有效性; 以及落实侵权救济和赔偿制度, 加强对信息处理者的监督与管理, 进而提供网络平台隐私政策中知情同意原则的破局思路。

关键词

知情同意原则, 隐私政策, 个人信息保护

The Dilemma of Applying the Principle of Informed Consent in the Privacy Policy of Network Platform and the Thought of Breaking the Point

Zhengyuan Han

Shanghai University, Shanghai

Received: Oct. 19th, 2022; accepted: Nov. 1st, 2022; published: Nov. 22nd, 2022

Abstract

As the imperial principle of personal information protection, the principle of informed consent it-

self has a profound legal basis, and the difficulties in its application cannot be used as a reason to shake the institutional structure. By investigating the practical dilemmas of the informed consent principle in the privacy policies of online platforms, and analyzing the causes of the difficulties in the application of the informed consent principle, on this basis, it is proposed to improve the performance of the obligation of informing by clarifying and simplifying the informed matters and adopting the form of marked notification. The privacy policy of "reasonable person" standard is constructed, and the dynamic consent mechanism and consent reversion mechanism are established to enhance the validity of consent, and implement the tort relief and compensation system, strengthen the supervision and management of information handlers, and then provide a breaking idea of the principle of informed consent in the privacy policy of network platforms.

Keywords

Informed Consent Principle, Privacy Policy, Personal Information Protection

Copyright © 2022 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 知情同意原则在个人信息保护中的存废之争

知情同意的概念最早由艾伦·威斯汀提出,是指任何组织或个人有权决定何时、何地以何种方式展示自己的信息[1]。知情同意在个人信息处理中分为知情和同意两个部分。知情即信息主体对信息处理主体收集、使用其个人信息的知悉,同意是指信息主体对信息处理主体收集、使用其个人信息的准许,知情是同意的前提和基础,同意又是知情的价值体现。知情同意已经成为世界各国个人信息保护的基础性原则,但在数字经济迅猛发展的今天,该原则却遭到越来越多的质疑声音。

1.1. 知情同意原则的质疑之声

在大数据时代,信息具有的社会价值被不断的放大挖掘,随之而来的是对知情同意原则的冲击与动摇。首先,个人信息的价值体现在于流动性,信息主体如要一直保持对个人信息的控制则要消耗巨大的成本和精力。其次,计算机、人工智能的不断发展,信息处理者对于信息的具体范围和内容往往并不能十分准确的知悉,更有甚者程序设计者也不知道算法黑箱是如何运作的,所以在这种背景下,又何谈对信息主体告知的准确性。另外,信息主体可能遇到的潜在风险,不仅仅在同意隐私政策收集个人信息阶段,还在后续信息处理、信息利用、信息加工、信息共享等各个阶段,因此风险是动态的,是伴随着信息处理的全过程。传统的个人信息保护模式只强调规制信息收集阶段存在的风险已不能适应如今的发展。

如今越来越多的声音开始质疑知情同意原则,是否还应该继续以知情同意原则来保护个人信息的安全。有学者认为,在数字经济蓬勃发展的潮流下,我们对于个人信息保护的立场并非严格保护而是防止恶意的信息处理者对个人信息滥用,否则不仅对信息处理者增加较高成本,而且信息主体也会消耗较多精力,降低信息流通效率,必然会降低信息产业的发展速度。我们可以通过设置删除权等方式对个人信息进行事后保护,进而取代形同虚设的知情同意原则[2]。甚至有学者直接指出,作为传统个人信息保护基础的“告知同意”已经失效,用户维权难度越来越大,并没有为用户的个人信息保护提供可靠保障,而且牵制了对数据价值的开发利用[3]。

总体而言，这些学者主张放弃知情同意原则，主要是因为它不能在大数据时代发挥自己的作用，这是一个实践适用知情同意原则的问题，而非其必要性与正当性的问题。一旦某项法律原则或规则难以适用，放弃它可能不是最明智的选择。毕竟没有十全十美的法律制度。目前，保护个人信息的最有效方式莫过于知情同意。在知情同意原则的前提下，探求更加合理的规则，提高原有模式下个人信息保护的有效性。

1.2. 知情同意原则地位之坚守

知情同意原则被誉为个人信息保护中的“帝王条款”，具有深厚的理论基础。虽然在大数据时代知情同意原则在实践中面临许多挑战，对个人信息保护也更加复杂难解，但我们不能执着于知情同意原则呈现出的困境，忽视其固有的价值，更不能一刀切地摒弃个人信息保护的这一根基。

1.2.1. 知情同意原则是保障信息相对自决的前提

个人信息自决权理论最早起源于德国，著名学者施泰勒认为信息自决权是人们可以根据自己的意志决定周围环境在何种标准下获得自己信息的权利。在大数据时代更加容易快捷获取信息主体的个人信息，信息主体控制自己的个人信息不被利用篡改实属不易，信息处理者对信息的获取和处理对信息主体而言很可能损害其利益。在这种情况下，清晰的告知和明确的同意非常重要。如果信息主体不能给予最基本的知情同意，保障个人信息自决权就是纸上谈兵。然而，知情同意原则仅是个人信息的前置保护，对个人信息自决权的绝对承认和保护并不是知情同意原则的价值追求。这是因为个人信息不仅具有个人价值，还具有社会价值的双重属性，同时，每个人对个人信息具有不同水平的认识，这就决定了受知情同意原则保护的信息自决权不是绝对的。

1.2.2. 知情同意原则弥补信息不对称差距

个人信息自决理论的目的在于解释个人信息处理为何要经信息主体同意，而信息不对称理论的意义在于解释信息处理者的告知义务和信息主体的知情权利。信息不对称情况的产生在于每个人掌握的信息的广度和深度是有差异的。在数据时代，自然掌握信息多的主体站在天平的高处，掌握信息少的主体便处于天平的低位。这种信息差的局面常常引发不公平的现象发生^[4]。对于信息主体与信息处理者两方面而言，无容置疑信息主体处于劣势，信息处理者凭借技术特长、资源优势拥有绝对的话语权。信息主体无法通过微弱的个人力量去洞悉信息处理者内部信息处理行为，因此也无法预料到信息处理的结果。为了修正双方不平等的关系，督促信息主体理性决策，真正拥有同意的权利，信息主体的知情权应落到实处，缩小双方信息差距，规避信息不对称对信息主体产生的损害。

1.2.3. 知情同意原则作为事前防范机制具有不可替代性

知情同意是作为个人信息处理的核心要件，知情同意原则已经成为世界各国个人信息保护中的重要框架和原则，在各国立法和实践中均有体现，是现有阶段为数不多形式上保障信息主体利益的措施。

个人信息安全保护实质上是一种风险预防，作为一种风险预防的机制，知情同意原则的存在不可或缺。信息主体和信息处理者之间风险更多的还是由信息主体承担，信息处理者只承担一种经营亏损、行政处罚等概括上的风险^[5]。用户作为风险承担者，有理由在充分知情的前提下被告知此类活动的风险和益处，进而预测和评估未来可能发生的风险，提前做好应对准备。同时考虑信息主体意志的参与，有利于给立法者提供平衡双方利益的参考，为个人信息的保护提供多样化的解决思路。信息主体提前预知风险并规避风险的权利由知情同意原则赋予。如果完全放弃知情同意原则，对个人信息的保护完全依靠事后防范，则会导致信息处理者更加肆意而为之，个人信息保护的路径将会进一步减少。

2. 网络平台隐私政策中知情同意原则的实践困境

用户同意网络平台隐私政策中的格式条款，网络平台处理信息主体个人信息，但伴随着算法等技术的出现，网络世界里的海量个人信息呈现流动的运作特点，信息处理规模不断变大，频率不断增强，由此放大了知情同意规则的局限性并演变为一种两难境地。

2.1. 信息主体知情权难以落实

对隐私政策中的重要事项知情是用户做出同意意思表示的前提，用户在充分知情的情况下所做出的同意是有效的，因此网络平台信息处理者的告知环节就极其重要，而目前网络平台的隐私政策对于个人信息保护而言早已形同虚设。

2.1.1. 瞒而不知：信息处理者告知不充分

网络平台在隐私政策中可能会将信息处理过程中存在的风险对用户隐瞒，误导辨认能力弱的用户同意隐私政策条款。信息处理过程中存在的风险，既包括泄露用户信息带来的危险，也包括通过大数据算法得出对用户不利的结果。在对常用的 10 款社交软件进行调查，有 6 款网络平台均表示会保障用户信息安全，不会发生信息泄露等损害用户的后果。只有今日头条、QQ、斗鱼、领英 4 款网络平台表明如果在技术或其他因素的影响下可能不能保证用户个人信息的安全^[6]。通常情况下，对于用户来说，基于网络平台往往是资质实力强的企业的信赖，潜移默化下会低估信息处理过程中存在的风险，而网络平台又通常将潜在的风险避而不谈，对用户没有履行充分告知的义务。尽管域外和我国均在个人信息相关法律中规定了“目的限制原则”，但该制度的实际运行情况差强人意。在大数据时代，可以将单条个人信息汇集起来经过算法而产生看似不相关事物之间的相关性，毫无疑问给用户带来潜在的危险。

2.1.2. 告而不知：隐私政策冗长晦涩

目前，各网络平台的隐私政策内容普遍较多，用语专业性强，并且相关政策经常被修改和调整。用户面对冗长晦涩的隐私政策束手无策，导致用户跳跃阅读甚至放弃阅读，信息主体的知情权难以真正得到有效保障^[7]。我们也可以从实证数据中看出隐私政策冗长晦涩的负面影响。有研究成果表明，如果信息主体粗读阅读提供给他们的所有隐私政策，那么每年需平均付出 154 个小时^[8]。这一“知情”的成本非常高昂。由于隐私政策复杂，阅读和理解的成本高昂，并且还会伴随无法预料的风险，网络用户选择对隐私政策条款视而不见是意料之中的事情。

2.1.3. 隐蔽告知：告知形式缺乏显著性

网络平台在设计隐私政策时会将关键信息置于位置不明显的地方，不加任何显著标识，这也是惯用的手法^[9]。2018 年，支付宝和芝麻信用合作，为用户推出了个性化账单服务，需要用户同意后才能生成账单，反映去年一年中消费者的消费情况。但支付宝使用的是年度账单首页左下角背景色附近的通知字体，字体较小，并且默认情况下勾选“同意”选项。在这种状态下，信息处理行为通过下滑动作自动启动，这就导致很多用户在没有看到告知内容就被动同意。¹关键信息位置隐蔽这种设计有何居心，在网络环境下，网络平台对隐私政策缺乏明显清晰的告知，屏幕之隔的用户又如何和网络平台进行约定授权。在冗长的隐私政策中让用户清晰了解自己的信息处理行为以及同意之后带来的后果，是我们必须解决的问题。

2.2. 信息主体同意有效性弱化

表意自由是信息主体做出意思表示的另一个先决条件。信息主体是自身利益的维护者，要提高同意

¹《国家网信办就“支付宝年度账单事件”约谈当事企业负责人》，载腾讯网，<https://tech.qq.com/a/20180110/005624.htm>。

的有效性就要确保信息主体能够真正按照自己的自身利益做出决定。然而，在现实中，处于劣势的信息主体只能接受隐私政策格式条款否则会影响使用网络平台，可见用户同意已经沦为一种形式。

2.2.1. 被迫同意：选择空间的缺乏

在现实中，网络平台和网络用户明显存在着地位的不平等，网络平台拥有信息优势，始终处于优势。对于用户来说面临两个选择，要么完全同意网络平台提供的隐私政策格式条款，要么拒绝网络平台提供的便利服务。比如支付宝、微信、网易邮箱这种 APP 已经和现代人的生活紧密联系在一起，因不同意隐私政策格式条款而放弃使用对于绝大多数人来说几乎是不可能的。因此即使用户知道默认同意的选项会有被过度收集资料的危险，也只能被迫同意。通常互联网大企业处于垄断地位，用户显然没有与其讨价还价的余地。看似同意是一个选项，实则是一个没有拒接的结果，此时用户的同意有效性大打折扣。

2.2.2. 同意架空：擅自许可第三方信息共享

信息的多次利用导致信息主体的同意被简化，成为不能保护个人信息安全的程序化摆设，网络平台在处理使用信息主体的个人信息过程中，为了追逐利益，可能会违反相关协议，超出约定的范围使用或擅自许可第三方使用。以北京淘友天下技术有限公司、北京淘友天下科技发展有限公司(两者系“脉脉”经营公司，统称脉脉)与北京微梦创科网络技术有限公司(系“新浪微博”经营公司，统称新浪微博)不正当竞争纠纷一案为例。²协议规定，新浪微博提供 Open API 协同发展模式，允许脉脉第三方平台通过 Open API 访问新浪微博平台数据，合作期限为一年，许可级别为“普通”。Open API 模式允许脉脉第三方平台在未经用户同意的情况下，通过相关界面访问用户的昵称、头像等信息。信息主体在同意时并无法预测其同意带来的后续影响，信息处理面临更大的风险，而且由于不适当的共享，知情同意框架被推翻。初始同意并不意味着信息处理者处理器可以自由处理用户的信息，无论初始目的的变更或者对第三方平台进行信息共享，信息主体的同意均失去对个人信息的有效保护。

2.3. 规则运行成本过高

知情同意产生的经济成本主要有两种：信息收集者为履行其告知和获得同意的义务而产生的成本，以及消费者为给予有效同意而产生的成本。

网络平台因知情同意付出的成本主要是“告知成本”，网络平台对隐私政策格式条款进行设计、调整、更新、传达所付出的经济成本。隐私政策不仅要符合法律要求还要符合国家政策，并且不同类型的互联网企业会根据本企业的业务类型以及营利目标设计自己的隐私政策，隐私政策也会随着法律法规、国家政策、企业目标等因素及时调整变更，因此会产生不少的合规成本。另外隐私政策的传播和回收需要投入巨大的时间和成本，随着用户的不断增加，网络平台处理海量的信息，成本必然会不断上升。

用户因知情同意付出的成本主要是“知情成本”，用户阅读隐私政策需要付出的时间成本。在微信、百度、支付宝等 8 款 APP 中，隐私政策的字数不少于八千字，篇幅长的达到近两万字。用户安装使用几十款 APP，需要阅读几十份冗长晦涩的隐私政策，用户投入的知情成本远远超出用户可承受的范围。

3. 网络平台隐私政策中知情同意原则适用困境成因

大数据时代，信息主体对于个人信息的掌控力在不断削弱，网络平台悄悄收集和用户的个人信息在用户并不知情的情况下。另外，信息主体受多种因素影响难以按照自己的自由意志给予有效同意。因此，即使信息收集者通过隐私政策获得了信息主体收集、利用个人信息的授权，这种授权是否真的真实有效？下文详细分析了造成知情同意困境的原因，并试图提供解决方案。

²北京知识产权法院(2016)京 73 民终 588 号民事判决书。

3.1. 隐私政策缺乏统一规范

为了满足充分告知和免除责任的要求,网络平台隐私政策通常将大量无关信息和关键信息混合起来,文字数量庞大,难以辨别有损用户的条款;倾向使用专业性强的词汇,使得隐私政策看起来繁琐且难以理解,用户因时间成本选择不看,或者基于看了也看不懂的心态直接跳过阅读选择同意,对于用户来说并非在真正知情的条件下同意隐私政策。

3.2. 敏感个人信息收集使用界限规定模糊

敏感个人信息是指如果被不法侵害,信息主体的财产或人身安全会遭受重大损害的个人信息总称。敏感信息与其他个人信息不同之处在于,侵犯敏感个人信息对用户产生的影响范围更大,损害也更难恢复。目前我国法律对一般个人信息和敏感个人信息的处理仅有原则性规定,细则并没有完善。因此现实中,绝大多数网络平台对一般个人信息与敏感个人信息的收集和处理并没有实质性的差异。但是网络平台对敏感个人信息和一般个人信息进行收集和处理时采用统一标准,没有区别化对待,实际上存在很大隐患。

3.3. 信息处理者缺乏有效监管

个人信息的价值并非来源于信息的载体而是信息的内容,正因为信息具有流动性的特质,不仅可以被信息主体掌握,信息处理者也可以掌握利用。对信息收集者缺乏有效监管,也是个人信息安全持续缺失的重要原因^[10]。

3.3.1. 行业自律规范性不足

严格执行告知同意原则只是保护信息的一小步,信息主体并不能对信息收集后的流转利用进行控制。个人信息的收集、处理、传输、利用等各个环节都存在被泄露的风险,如果只基于用户自身的防范意识和网络平台的自觉性,并不能有效的保护个人信息。与此同时社会也必须成为保护个人信息的责任人。数不胜数的企业已经洞悉利用个人信息来发财致富,网络平台良莠不齐,由于缺乏统一的行业标准,绝大多数企业都不能抵御诱惑,降低企业标准,以用户个人信息为对价换取财富。

3.3.2. 缺乏事前事中有效监督

对于侵犯个人信息的法律规制,我国多是以事后监管为切入点,缺乏有效的事前和事中监管。一旦缺少事前统一审查,不遵守规则的网络平台将会进入市场,由此引发用户信息泄露等危险。在信息处理的中期缺少监督,个人信息在流通交易情形下极易遭受侵害。目前专业监管个人信息保护的机构还未设立,不同行业的监督部门相对分散,监督主体职责存在不明确、相互推诿的现象,不重视用户信息保护问题,就导致对网络平台用户个人信息二次利用的监管不足,信息监管体系并不能系统完善的建立起来。

3.4. 信息主体维权救济困难

我国对个人信息权的界定尚不明确,对个人信息侵权责任的构成要件、赔偿等没有专门规定,司法实践中通常采用一般侵权责任的构成要件,这就表明,更多的举证责任是由被侵权人来承担^[11]。现实生活中,网络平台用户个人信息被侵害,被侵权人的法律意识不足,维权能力有限,网络平台用户处于劣势地位。而作为侵权一方的企业通常资金实力强,享有较高的社会知名度。采取一般侵权责任的举证规则,就会显失公平。

3.4.1. 举证困难

随着信息技术的不断发展,侵害个人信息方法的隐秘性也在不断增强,用户很难察觉网络平台在何

时以何种方法泄露自己的信息，等到侵害结果发生后才恍然大悟，因此用户很难确定真正的侵权人。信息处理存在诸多程序，用户仅能掌握信息收集前的过程，对于后续的流转就难以控制。网络用户并不具有相关领域的专业知识，个人信息经过算法处理后，必然导致被侵权人无法确定侵权行为的具体责任人。即使用户能够找到具体的侵权人，也不能证明侵权人对信息泄露存在过错责任，且侵权行为与损害结果之间存在因果关系。用户没有确凿的证明支撑自己的举证，想要拿到胜诉的结果是很难的。

3.4.2. 损害赔偿力度小

我国司法实践中对于侵犯个人信息的案件，确定侵权责任和损害赔偿的大小主要是依据《民法典》侵权责任编的规定。由于侵犯个人信息行为所造成的损害不易发现，很难依靠侵权行为推断和预测损害结果，因此明确的损失数额是难以确定的。网络平台用户个人信息被侵害，不仅会造成财产损失，还会造成其他损失。而且各地法院对损害程度的判断没有统一标准，被侵权人更难获得赔偿和补救[12]。当事人已经通过各种办法积极维护自己的权利，最后的结果往往救济力度不大，可能还会面临败诉的风险，大多数人最后都会选择大事化小，小事化了。

4. 网络平台隐私政策中知情同意原则的脱困思路

在国家、企业(数据控制者和数据处理者)和数据主体构成的个人信息控制和处理的三方结构中，信息主体不光是在获取信息的能力和亦或是保护自身利益的能力，各方面都处于劣势地位，因此，保护个人数据的基本价值观念不应建立在牺牲个人信息保护的基础上，而应将保护和使用个人信息作为最基本的理念加以衡量[13]。尽管知情同意原则在个人信息保护中面临困境，但告知同意原则仍有其合理性，其在个人信息保护中的地位不能动摇。因此，如何充分发挥知情同意原则的效力，有效平衡当事人的利益关系就成为一个亟待解决的问题。

4.1. 完善告知义务履行

网络平台对用户个人信息的收集和处理应采用公开、透明的方式，信息主体对于信息收集目的、方式、范围等事项享有充分的知情权。从现状来看，用户因网络平台形式化的告知能不能获得真正知情。知情权和同意权作为消极性权利，实现的前提是网络平台充分履行告知义务[14]。因此，若要加强知情同意原则，对于告知的形式应当规范，并确保其真实、全面和可理解。

4.1.1. 明确和简化告知事项

简化告知形式和保证告知内容全面丰富两者并不存在对立，隐私协议内容的丰富离不开知情同意原则的规范，告知内容的优化在一定程度上是依靠简化告知事由而实现的。想要隐私政策简单明了，可以采用两个版本来实现。第一个是详细的全文版，第二个是精简版，具体告知三类事项即可，即“收集的目的与范围”、“收集处理的规则和方式”、“用户同意或者拒绝可能产生的后果”，重点向用户告知第三个事项，明确提醒网络平台用户未来潜在的风险。

4.1.2. 显著标识告知形式

隐私政策中晦涩难懂的条文，网络平台可以将其转化为图片形式，图片和文字相结合是一种显著、简单易懂的提示方式。除此以外，还可以对关键信息使用彩色字体，加入下划线，采用窗口弹出等方式提醒网络用户对相关事项加强重视，谨慎阅读。并对隐私政策中的专业术语通过添加链接的方式对其进行清晰说明。

4.1.3. 对隐私协议条款进行规范

网络平台提供的隐私政策格式条款是否合法，有关部门应当事先进行审查。另外，相关的行业协会

可以制定统一规范的示范条款供网络平台设计隐私政策参考[11]。如果隐私政策的格式条款明显有害于网络平台用户，不合理加重用户责任，对信息处理者的责任给予减轻，则该隐私协议不能成为信息收集者免责的事由。

4.2. 增强同意的有效性

严格遵循告知同意原则，对于提高网络平台用户信息安全保护意识，增强用户对个人信息的控制力具有重要意义。但现实存在的隐私政策冗长晦涩，完全违背了告知同意的初衷。不仅降低了用户体验感，也使用户同意的有效性弱化。想要提高用户同意的真实性，就要调整现有的同意方式。

4.2.1. 构建“理性人”标准的隐私政策

网络平台用户做出同意的前提是充分意识到个人信息的收集、使用和流通的情况，在这种条件下用户的同意才是真实的。知情程度不仅受网络平台告知义务的履行程度影响，同时用户自身的不理解力也会对知情产生影响。网络平台用户的信息理解力通常是由年龄、专业知识、社会经验等方面共同决定的，因此每个人生活背景、工作经历不同，对信息的理解程度也是不能相提并论的。而网络平台不可能针对不同理解能力的人单独订立隐私协议格式条款，因此判断当事人是否知悉，应该把具体信息内容作为依据，以一般理性人能否理解作为隐私政策格式条款设计标准。

4.2.2. 建立动态同意机制

以往的知情同意方式一锤定音，没有考虑未来怎么样，在这种情况下签署隐私协议既是同意的开始，也是同意的结束。在实践层面上，个人信息的收集、利用是动态的过程，随着大数据经济的快速发展，信息流转、超出同意范围使用、再次利用等等现象屡见不鲜，知情同意模式已经不能满足现状。网络平台用户对个人信息的后续处理情况不得而知，失去对个人信息的控制权是必然的，更不用说信息自决了。个人信息仅靠事前概括同意并不能产生有效的保护，当相关情况发生变化时网络平台应保持动态披露。用户若拒绝同意隐私政策，网络平台还应提供拒绝通道和撤回同意的渠道。在操作上，网络平台应为用户保留退出权，用户对个人信息的更新变化可以及时了解，以此为根据主动地给予或撤回同意。

4.2.3. 建立同意撤销机制

建立同意撤销机制，目的在于赋予信息主体同意撤销的人格自治利益[15]。首先，无论是因为超范围收集信息，还是信息处理过程中存在对用户不利的影响，亦或是用户信息被第三方平台利用的风险，一旦个人信息安全风险爆发，风险的终极承担仍是网络平台用户个人。发生上述情形之一的，为使用户的损害降到最低，用户可以在同意授权后做出撤销授权。其次，建立同意撤销机制，可增强网络平台对用户个人信息保护的重视程度，督促其谨慎收集利用，网络平台用户的劣势地位在一定程度上可以改善。同意撤销机制的还应具体规定和限制以平衡网络平台与用户之间的利益，网络平台一旦收到用户的撤销同意通知，就应当停止信息收集行为并删除此前收集的信息。网络平台应为用户行使同意撤销权提供便利条件，如在应用权限设置中增加撤销途径，在隐私政策中明确用户享有任意撤销同意的权利。

4.3. 落实侵权救济和赔偿制度

“谁主张，谁举证”是我国民事诉讼领域普遍适用的举证规则，但在网络平台侵害用户个人信息的案件中将举证责任分配给处于劣势的用户则是显失公平的。在大数据时代，传统的个人信息保护规则已经无法适应当下形势。

4.3.1. 实行举证责任倒置

网络平台负责信息收集和处理，和用户比较而言无疑处于优势地位，应当承担更多的举证责任。实

行举证责任倒置有利于实现诉讼主体地位的平等。网络平台应证明在收集处理信息的过程中已经充分履行了保护用户信息安全的义务，没有过错责任。用户只需证明存在侵权损害行为和损害后果。降低用户的举证责任，不但有利于用户积极维权，而且对与存在不良企图的网络平台具有威慑力，在诉讼中给予用户第二层保护。

4.3.2. 加大侵权损害赔偿力度

在大数据时代，信息资源的价值愈发突显出来，网络平台在衡量巨大的利益诱惑和较低的违法成本后，往往会铤而走险。明确的个人信息侵权救济赔偿制度以及加大个人信息侵权损害的赔偿力度，对于网络平台谨慎设计隐私政策，减少个人信息侵权事件发生具有威慑力。

4.4. 加强对信息处理者的监督与管理

建立个人信息的监管体系，不仅需要政府参与，网络平台以及所在行业也应成为监管体系中的一员，形成政府主导、部门配合、公民广泛参与的监管机制。

4.4.1. 信息主体增强个人信息保护意识

对于个人信息的保护，网络平台用户也应增强安全意识，不能放松警惕。应当通过安全正规的途径下载使用软件，仔细阅读隐私协议中的条文，如有不理解的地方可以自行查询或与平台联系。定期清除浏览足迹，不要随意在网络平台上授权或输入个人信息。如果发现个人信息被网络平台非法泄露和利用，及时寻求法院等部门帮助，维护自己利益。加强网络平台用户自身的监督责任感，从而强化网络平台按照法律规定和国家政策收集使用用户个人信息。

4.4.2. 建立事前预防、事中监督、事后追踪的统一监管体系

监管机关的监督职责和监督范围要明确，建立专门监管个人信息的机关，形成事前预防、事中监管、事后跟踪的全方位监督体系，为用户的个人信息安全保驾护航[16]。所谓事前预防，就是有效审查网络平台隐私政策的告知方式，防止形式化的知情同意发生；事中监管，就是对网络平台收集、处理、利用、流转用户个人信息的环节进行风险评估和监督，减少低用户信息被未授权的第三方平台收集使用。事后跟踪，就是当用户的个人信息被非法侵害时，及时使当事人知情，阻止损害的进一步扩大，并为当事人提供法律援助。

4.4.3. 加强行业自律

不同行业会有不同的行业内部专业知识，对于个人信息的收集利用规则也是大相径庭，行业内部更有可能发现目前行业个人信息规制存在的问题，对症下药制定出合适的监管制度，因此建立行业自律组织对行业的监管是大有裨益的。提高企业的风险意识和遵纪守法态度，行业内部相互监督，动态监测企业有无非法收集利用用户个人信息，不定期检查，打造安全健康的行业氛围。

5. 结语

在大数据时代，个人信息的价值被挖掘出来，个人信息已经成为重要的社会资源。网络平台利用用户的个人信息获得巨大的利益，与此同时信息主体的人身和财产权益受到损害。个人信息保护不仅立足于保护用户的私人利益，也将社会公共利益和商业利益包含在内。关于如何平衡三者之间的利益关系一直争论不休，是我们必须直面的问题。

知情同意原则是网络平台对用户信息收集前的事先授权，目的在于降低非法收集利用用户信息的风险。我们从实践中看出，隐私政策中形式化的知情同意原则运用的有效性并不高，用户的知情同意被架空，适用成本较大，用户举证维权困难，网络平台监管薄弱，信息主体很难保护自己的权利。但是运用

效果不理想并非只有放弃知情同意原则这一条路可以走,改进完善知情同意原则可以使其发挥出更好的效用。可以预见,知情同意原则的形式化正在不断修正,用户的权利救济路径也在不断拓展,信息监管体制能够最终建立。经过法律的不断完善和实践的屡次检验,知情同意原则的困境将会一步一步打破。

参考文献

- [1] 江帆,常宇豪.个人信息保护中“知情同意”适用的困境与出路[J].经济法论坛,2018(2):46-64.
- [2] 任龙龙.论同意不是个人信息处理的正当性基础[J].政治与法律,2016(1):126-134.
- [3] 范为.大数据时代个人信息保护的路径重构——初探欧美改革法案中的场景与风险理念[J].网络信息法学研究,2017(1):248-286,393-394.
- [4] 张维迎.博弈论与信息经济学[M].上海:上海人民出版社,2004:397.
- [5] 姚佳.知情同意原则抑或信赖授权原则——兼论数字时代的信用重建[J].暨南学报(哲学社会科学版),2020,42(2):48-55.
- [6] 陈瑞华,郑洁萍.在利益与人格之间:社交网站个人信息保护研究——基于10家社交网站的分析[J].新闻界,2018(5):46-54.
- [7] Ben-Shahar, O. and Schneider, C.E. (2011) The Failure of Mandated Disclosure. *University of Pennsylvania Law Review*, 159, 658-665. <https://doi.org/10.2139/ssrn.1567284>
- [8] McDonald, A.M. and Cranor, L.F. (2008) The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society*, 4, 563-568.
- [9] 林凯,张建肖.知情同意权的功能失灵与应对——兼评《数据安全管理办法(征求意见稿)》相关规定[J].中国应用法学,2020(2):162-186.
- [10] 时明涛.大数据时代个人信息保护的困境与出路——基于当前研究现状的评论与反思[J].科技与法律,2020(5):66-74.
- [11] 王利明.数据共享与个人信息保护[J].现代法学,2019,41(1):45-57.
- [12] 陈吉栋.个人信息的侵权救济[J].交大法学,2019(4):40-53.
- [13] 丁晓强.个人数据保护中同意规则的“扬”与“抑”——卡-梅框架视域下的规则配置研究[J].法学评论,2020,38(4):130-143.
- [14] 宁园.个人信息保护中知情同意规则的坚守与修正[J].江西财经大学学报,2020(2):115-127.
- [15] 陆青.个人信息保护中“同意”规则的规范构造[J].武汉大学学报(哲学社会科学版),2019,72(5):119-129.
- [16] 褚宏俐.个人数据利用与保护的法律问题研究[J].宁波广播电视大学学报,2019,17(4):58-64.