Dispute Settlement 争议解决, 2021, 7(1), 8-15
Published Online March 2021 in Hans. http://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2021.71002

Hans汉斯

个人信息处理：重新审视对同意原则的适用

孙心依

华东政法大学，上海
Email: thecoolxinyi@sina.com

收稿日期：2021年1月23日；录用日期：2021年2月23日；发布日期：2021年3月2日

摘　要

在我国当前的个人数据保护立法框架下，同意原则是个人数据处理的首要合法性基础，其他合法性基础被设置为“同意的例外”。但随着数据领域的快速发展，同意作为个人信息处理的必要前提出现了越来越多的问题和局限。本文将基于比较法的角度，研究中国香港、菲律宾、欧盟、美国加州这几个司法辖区的个人信息保护立法中对同意原则的适用情况，探究同意与个人信息处理行为之间的逻辑关系，并与我国个人信息保护立法中的相关立法进行比较，研究同意原则应当被如何适用，才能有利于我国个人信息治理体系的有效性和稳定性。

关键词

个人信息处理，个人信息保护，同意原则

Revisiting the Role of Consent in Personal Data Processing

Xinyi Sun

East China University of Politic Science and Law, Shanghai
Email: thecoolxinyi@sina.com

Received: Jan. 23rd, 2021; accepted: Feb. 23rd, 2021; published: Mar. 2nd, 2021

Abstract

In the context of China’s data privacy framework, consent plays a leading role in legitimizing the processing of personal data, while other bases of lawfulness are set up in the form of “exceptions to consent”. However, with the continuing improvements in data science, the effectiveness of consent as the necessary prerequisite for data processing is increasingly being called into question. This paper will study the role of consent in the data privacy framework of different jurisdictions,

文章引用: 孙心依. 个人信息处理: 重新审视对同意原则的适用[J]. 争议解决, 2021, 7(1): 8-15.
DOI: 10.12677/ds.2021.71002

including Hong Kong, the Philippines, EU, and California, to explore the logical relationship between consent and the processing of personal data, and then compare it with the relevant legislation in China to figure out the role of consent in legitimizing the processing of personal data.

Keywords

Processing of Personal Data, Personal Data Protection, Consent

1. 问题的提出

随着大数据的不断发展，个人信息保护及其立法在世界范围内引发热潮。而在这些个人信息保护立法中，往往用“个人信息处理”行为涵盖个人信息的收集、披露、共享、传输及转让给第三方的行为。中国目前尚未发布关于监管个人信息处理的国家级法律，但 2012 年全国人大常委会通过的《关于加强网络信息保护的决定》首次在法律层面将信息主体的“同意”作为个人信息处理的合法性基础；《中华人民共和国网络安全法》明确网络运营者收集、使用个人信息必须取得个人同意；《数据安全管理办法(征求意见稿)》在坚守同意规则的基础上，对同意形式进行限定；《信息安全技术个人信息安全规范》(2020 版)也规定个人信息收集、使用原则上必须征得数据主体的“授权同意”，如果是敏感信息，还必须得到个人数据主体的“明示同意”；2020 年 10 月 21 日公布的《个人信息保护法(草案)》(以下简称“《草案》”)将同意作为个人信息处理中的最基本规则。从上述的法律规制可以发现，我国目前仍然将同意原则视为几乎所有个人信息处理行为合法的必要前提，至少在《草案》及其起草者的思维模式中，“同意”被置于各类数据处理的中心位置——将“同意”当成了个人信息处理行为的必要前提的同时，将其他事由处理成“例外”情况。

“同意”原则也被称为告知同意原则，是指数据的收集者将其收集到的个人信息公开、共享、传输或者转让给第三方时，应当对信息主体就有关个人信息被收集、处理和使用的情况进行充分告知，并征得信息主体明确同意的原则。在这一原则下，只有数据主体本人才有权决定是否提供其个人信息及其信息可被利用的方式。同意原则在全球范围内的个人信息或隐私保护立法中被普遍适用，被赋予现代数据保护法的“核心”、“首要基础”的地位。

但是，通过比较法考察可以发现，尽管各个司法辖区的个人信息保护立法几乎无一例外地规定了该制度，在不同法域中，同意与个人信息处理之间的逻辑关系却相差甚广。本文将基于比较法的角度，研究中国香港、菲律宾、欧盟、美国加州这几个司法辖区的个人信息保护立法中对同意原则的适用情况，探究同意与个人信息处理行为之间的逻辑关系，并与我国个人信息保护立法中的相关立法进行比较，以寻找对具体问题的解决方案。

之所以选择上述司法辖区，是因为它们代表了个人信息保护立法的不同阶段：欧盟《通用数据保护条例》(General Data Protection Regulation，以下简称 GDPR)和美国加利福尼亚州的《加州消费者隐私法》(California Consumer Privacy Act，以下简称 CCPA)代表了拥有相对良好的个人信息保护秩序的司法辖区对个人信息保护的两种不同思路；菲律宾法律于 2016 年颁布，受到 GDPR 的影响，却又存在相当程度的本地化改造；我国香港地区的个人信息保护立法是亚洲最早的成文法之一，已经实施了 25 年，形成了较

为完善的解释体系和执法程序；我国内地的个人信息保护则起步较晚，目前尚未出台专门的个人信息保护法，而从目前《草案》公布的内容看，在一定程度上借鉴了欧盟 GDPR 的立法模式。

2. 不同司法辖区“同意”与个人信息处理的逻辑关系

从比较法的角度看，不同司法辖区的个人信息保护立法对同意与个人信息处理之间的逻辑关系具有不同的理解。总体看来，不同司法辖区中“同意”与个人信息处理间主要有以下三种逻辑关系：

2.1. “同意”被作为个人信息处理的合法性基础之一

不论是早期的《个人数据保护指令》(95/46/EC)还是近期的 GDPR，欧盟的个人信息保护立法一直格外强调“同意”对于个人信息保护的意义。GDPR 第 6.1 条“数据处理的合法性”(lawfulness of processing)列举了数据控制者可以合法处理个人数据的六种情况：1) 数据主体已经对基于一个或多个具体目的而处理其个人信息的行为表示同意；2) 为履行或达成合同，且个人数据主体是(或将成为)合同的一方当事人，所必要的数据处理；3) 为履行数据控制者的法定义务所必要的数据处理；4) 为保护数据主体或另一自然人的重大利益所必要的数据处理；5) 对履行涉及公共利益的职责或实施已经授予数据控制者的职务权限所必要的数据处理；6) 数据控制者或第三方为追求合法利益目的而进行的必要数据处理。

从逻辑关系上来看，GDPR 一方面将“同意”放在突出的位置，另一方面似乎并不完全信任其是否适合保护数据保护所涉及的利益：首先，GDPR 第 6 条列举的六项合法性基础之间属于并列关系，无先后之分，只要满足(1)至(6)项中的任意一项规定，即具备了个人信息处理的一般合法性基础。其次，在任何情况下，即使数据主体已合法同意处理，控制者不仅必须采取适当的安全措施，以维护所收集数据的完整性，而且还必须限制处理过程中产生的风险。数据控制者必须评估这些风险，并在某些情况下进行数据保护影响评估(GDPR 第 35 条)。第三，它严格规范同意，规定同意必须符合严格的要求。最后，它排除了在某些情况下可以基于个人同意进行处理，如果情况不允许自由表达，则不能援引同意(GDPR 第 29 条)。

2.2. “同意”被作为个人信息处理的必要前提条件

菲律宾《数据隐私法(2012 年)》(DPA)从措辞和立法体例都受到 GDPR 的很大影响，但又存在相当程度的本地化改造。合法处理个人数据的情况在 DPA 的第 12 条被列出，包括：1) 数据主体已经给出特定形式的同意；2) 为执行或准备与个人数据主体的合同而必须进行的数据处理；3) 为保护数据主体的生命及健康而必须进行的数据处理；4) 为实现公权力机关合法的非商业目的，而必须进行的数据处理；5) 为了医疗目的而必须进行的数据处理；6) 为履行数据控制者的法定义务所必要的数据处理。

单从 DPA 第 12 条的措辞来看，这六种合法处理数据的情况与 GDPR 第 6.1 条中的六项合法性基础颇为相似。逻辑上似乎也借鉴了 GDPR 第 6.1 条，即数据主体的同意是所有数据处理行为合法化的六种合法性基础之一，与其他五种相并列。然而，DPA 并未在全文中保持这一逻辑，第 32 条的罚则又做出了如下规定，“任何个人信息控制者和个人信息处理者，在没有得到个人数据主体的同意的情况下向第三方披露个人信息，应当被处以 1-3 年监禁，并处 50 万-100 万比索的罚金。”在这一罚则下，前述第 12 条规定中的六种合法性基础仅适用于除共享数据外的其他数据处理行为，数据控制者若要向第三方共享数据，获得数据主体的同意将是唯一的合法性基础。DPA 的第 25 条也表明：个人信息共享行为与一般的数据处理行为被分开对待：对一般的数据处理行为而言，该法规定了两类合法性基础：一是个人数据主体的“同意”，二是“本法规定的其他情况”。而个人信息共享行为就只有一个正当性基础——即数据主体的同意。

可见，DPA 第 25 条和第 32 条的规定显然第 12 条的逻辑不相吻合，前款还将“同意”被作为个人信息处理的合法性基础之一，后款却规定个人信息共享行为只有数据主体的同意这一个合法性基础。因此，菲律宾的个人信息保护立法仍然将“同意”作为个人信息共享合法的不可或缺的必要条件。

2.3. “同意”并非个人信息处理的合法性基础

在以香港和美国加州为代表的第三种模式下，“同意”被限制在了一个次要的位置。

香港《个人资料(私隐)条例》(PDPO)是亚洲最早制订的全面个人信息保护法，根据经合组织 1980 年《关于保护隐私和个人数据国际流通的指南》起草，于 1995 年通过，并于 1996 年 12 月生效。PDPO 至今已经实施了二十五年，形成了较为完善的解释体系和执法程序。

根据 PDPO，一般而言，“资料使用者”(与 GDPR 中的数据控制者相当)无需在收集和处理个人信息之前征得个人数据主体的同意。只有在例外的情况下，才需要获得用户的同意。例如，商家利用个人资料进行“直接促销”前，需要获得“订明同意”。在个人信息处理方面，资料使用者也不需要专门获得用户的“同意”，而只需要满足“通知”义务——在其《个人资料收集声明》阐明将如何处理获得的数据即可。此后，如果其处理行为在声明所说明的范围内，则符合法律的规定。简言之，香港法律在个人信息处理领域采取的是通知注意。“同意”并非个人信息处理的前提。

在美国，数据保护立法有以下特点：“一是鼓励信息的自由流动；二是有限的隐私期待；三是实质损害利益平衡；四是以行业自律为主”[1]。因此，同意在个人信息保护立法中并不具有基础地位，更不是一项法律原则，无需同意或默许同意的情况普遍存在。以美国加利福尼亚州颁布的《2018 年加州消费者隐私法案》(CCPA)为例：根据 CCPA，与“个人信息处理”对应的概念是个人信息的“销售”——被定义为：“金钱或其他有价值的考虑、出售、出租、发布、披露、传播、提供、转让，或以其它方式通过书面、电子或其他形式将消费者的个人信息传输给其他人。”

为了使“个人信息处理”合法化，原始数据的收集和控制者必须向数据主体提供“选择退出”的机会。在默认情况下，如果数据主体再看完通知后，没有做出“退出”或者“拒绝销售”的选择，则其个人信息就可以被提供给第三方。可见，CCPA 并未将“同意”作为数据处理或个人信息共享的先决条件。相反，即使在为营利目的处理个人信息的情况下，对“同意”的要求也是通过“选择退出”的方式实现——在默认情况下，假定用户是同意的。这一模式也给予数据主体随时要求数据控制者“不准卖”其个人信息的权利，使数据控制者很难再将同意出售个人信息打包在其他个人信息使用许可中，使消费者只能“一揽子”的接受。

综上，美国和香港的法律表明，在一个良好的个人信息保护秩序中，另一种数据保护的思路是“同意”不仅不需为数据处理的必要前提，甚至无需作为一个前提条件。

3. “同意”作为信息处理必要前提的利弊分析

个人数据主体的“同意”究竟应当在个人信息处理的规范体系中居于什么位置？很大一部分学者认为设置“同意”规则是确保个人对其信息自主权的最佳方式，能够最大程度地捍卫个人尊严和行动自由，因此应当是数据处理最重要的法律基础[2]。这一论点基于两个主张。第一，数据保护的发展方式很大程度构成了同意的重要性。保护个人信息的权利被《欧洲基本权利》宪章(第 8 条)定义为一项基本权利，因此，欧洲立法者将数据保护塑造为个人权利的主体，从而将其引向人格权的领域，而人格权实际上就是个人的权利。其基本假设是，数据属于其所指的个人，因此，处理数据需要得到个人同意。第二，“同意”的综合效果是在个人信息处理的利益和风险之间达到平衡——在个人信息被处理之前，若数据主体点击了同意，那么他就可以得到比不同意分享信息的用户更好更多的服务，同时也冒上更多个人信息被

泄露的风险。由数据主体自己决定是否用自己拥有的信息换取利益，从逻辑上来看似乎顺理成章。

但是，如果进一步审视“同意”的逻辑，就会发现将其作为合法的个人信息处理的必要前提，存在一定的问题和局限。

3.1. 同意与数据主体自主权的关联度较低

首先，在实践中，个体的同意并不完全可靠。同意与数据主体的自主性关联度较低[3]，而自主性恰恰是“同意”的前提和结果。数据主体的认知偏差和心理活动，加上人口、文化和种族特征，都会影响到给予或拒绝同意的复杂过程，使得“信息自决”沦为“信息他决”，这使得用户的同意决策与数据接收者的承诺弱关联。从这个角度看，同意是不充分的，因为个人没有条件给予完全知情的同意。

其次，大数据降低了个体同意的价值。大数据技术特别具有侵入性，因为它们能够从看似无害和相互关联的数据中创建详细的档案。它本质上依赖于收集大量的个人信息，并将其继续用于收集数据最初用途以外的目的。每个具体的个人向数据控制者表达同意的意愿时，很少会弄清自己的哪些数据将如何被数据控制者处理。大多数用户的资源和能力也很有限，无法验证处理是否在其同意的范围内，更不用说这些个人信息共享给第三方后的处理情况了。随着时间的推移，数据主体可能进一步丧失同意的自主权[4]。同时，大数据时代信息的处理量空前巨大，越来越多的人认为，规定每次使用个人信息都必须征得明确的同意已经不切实际。综合上述因素，同意(即使是完全知情的、具体的、不存在限定的权力失衡)不能构成处理的合法基础[5]。

3.2. 个人信息所有权并不归属于数据主体

所有权一般是指“在不与法规或第三方权利发生冲突的前提下，允许权利主体使用、管理和享有财产的权利，包括将财产转让给他人的权利”。基于这一定义，私有财产的处置应当完全基于财产所有者的决定。在“数据主体拥有个人信息所有权”的假设上，将“同意”作为数据处理必要前提似乎具备法律基础。但这种将个人信息认定为数据主体所有权客体的假设显然已经受到了不少学术界的挑战：隐私学者 Daniel J. Solove 认为鉴于“隐私”范围不明确，且内容一直在变动，因此很难被明确定义，也就不可能将其认定为所有权的客体；Lothar Determann 在《没有人可以拥有数据》一文中指出，美国和欧盟法律对数据所有权的概念均持反对态度。个人、企业、政府和公众对数据和使用均享有不同的利益，而单一化的数据所有权将无法促进对隐私的保护，甚至可能阻碍言论自由、信息自由、和科技的进步。笔者进一步认为，个人信息之所以不可能受到单一所有权的约束，是因为这些信息一直处在不断的变化中：一组个人信息从产生到存储，再到被聚合、分解和重组，几乎每次数据处理都会产生新的数据，而产生这些新数据的产生并非基于数据主体的主观意志，而是数据处理过程中的外溢效应。在客体都无法固定的情况下，不可能在这种客体上施加所有权，因此，所谓“某个人的信息”，实际上指的是“可以用来查找、定位某个人的各种信息”或者“与某个人的身份有关的各种信息”，这些信息集合在一起，形成了一个人的社交肖像(social profile)，这种社交肖像伴随着人在社会中的每一个行动而不断发展，是他人用于识别个体身份的信息，与个体的身份是不同的概念。用来识别身份的信息实际上不可能、也不应该被数据主体拥有和控制，否则的话，个体将可以随意变化身份。

再者，个人信息保护和隐私领域的工作不仅需要评估“同意”的数据处理对个人利益的影响，还需评估其在社会方面的影响。因为当代对所谓“个人”数据的处理意味着一种不再是双边的模式，不仅涉及数据主体和控制者的利益，更涉及到第三者的利益及社会公益。正如 J. Cohen 所指出的，“隐私的概念已经远远超出了个人同意的范围，正在被重新概念化为出于个人福利之外的原因而受到保护的社会公益。”[6]例如，Facebook 部署的面部识别系统的争议说明了当涉及医疗数据，特别是基因数据时，个人

信息的处理可能会对家庭成员产生影响。而从更广泛的角度来看，第三者可以泛化为整个社会，个人信息相关技术发展带来的风险包括社会控制、歧视、监视、社会顺应、隔离和排斥少数群体等方面，而这些风险均具有集体性，涉及整个社会，而在劳东燕教授和高富平教授看来，采用以同意机制为主的模式来保护个人信息，就等于是将这些数据的风险主要放在作为数据主体的个人身上。因此，个人信息的处理不应完全由个人同意来决断[7]。

3.3. 同意原则可能被用以规避数据保护的责任

当法律将“同意”作为数据处理的必要前提时，无意中逼迫数据控制者与数据主体之间变成了竞争而非合作的关系。在以达成“契约”为目的的法律关系建立过程中，它们作为合同的相对方，必然消耗大量的时间和精力去防止对方的违约行为——在什么算同意，是否已经同意以及如何证明同意行为的发生等问题上，耗费精力和成本。

数据控制者与数据主体的对立关系似乎不可避免，但过分强调这种对立关系，恰恰为恶意的数据窃取者或者聚合者提供了获利的空间。当发生大规模侵害个人信息的行为时，数据控制者与数据主体都把时间和精力用在指责对方身上，忙于相互推卸责任，而忽视了数据滥用的深层次原因和那些真正作恶的数据窃取者或者搭便车者(例如在 Facebook 或者其他社交平台提供者例如“剑桥分析公司”或者一些滥用数据对监控他人的机构)。

另外，当法律强制性地要求“同意”作为数据处理的必要前提时，就等同于让数据控制者以追求同意为目的，实际上造成了手段与目的的倒置。数据控制者会自然地将资源投入到鼓励用户“同意”上，而非投放到增强其保护用户信息的能力上。因为只要获得了用户的同意，并且将这种同意的证据固定下来，数据控制者至少已经在行政监管层面过关。而用户要证明其当时的“同意”是在未获得充分通知、或者是在未能明确个人信息的披露范围的情况下做出的，这涉及困难的证据搜集步骤：用户要证明的是自己“没有同意”——而让人证明自己“没有做某件事”的难度远远大于证明其“做过某件事”。

在这个背景下，作为商家的数据控制者将失去实施内部控制、避免个人信息被滥用的动力。相反，他们会将精力集中于找到合规的途径，例如将用户条款或者隐私权政策中的措辞复杂化或悄悄扩大或者模糊“同意”的范围，并以用户点击“同意”的记录作为免责的尚方宝剑。2007 年，著名的隐私学者 Christopher Kuner 曾建议企业“减少依赖于同意而获得行为的合法性。”而这个建议对立法者也同样适用，毕竟，好的法律应当让善意的受调整方的利益趋向一致，共同创造美好的秩序，而非刺激他们规避责任，或为了各自的利益互相争斗，增加交易成本。

4. 思考与改进:“同意”应当被如何定位

根据上文的论述，将同意原则作为个人数据处理的必要前提在实践中已经证明了弊大于利：不仅在所有权上缺乏法理支持，且数据主体的同意自主权也易受干扰，更有可能被数据控制者滥用。对此，加州大学伯克利分校法学院的 Paul M. Schwartz 教授和德国科隆大学的 Karl Nikolaus Peifer 教授曾在他们合著的文章中指出：“我们已经预计到无边界地采用同意和契约原则所带来的后果，欧盟建立了一套新的数据保护法律规则，正是为了改变建立在‘同意’和‘契约’原则上的数据保护路径，将这些契约放入特定轨道以限制他们的适用。”[8]可见，GDPR 是对过度依赖“同意”原则做出的矫正，它的一个重要作用就是限制了同意原则在数据保护上的适用范围。美国作为个人信息保护秩序良好的司法辖区，其数据保护法律体系则从一开始就弱化了强调了数据主体对数据处理的“同意”作用，而强调“通知”和“披露”的重要性，有效地打击了数据市场中的欺诈和不公正。从这个角度看，我国数据保护法律体系与欧盟相近，而与美国的隐私权体系相差甚大，虽然没有必要借鉴美国的数据保护观点，但也没有必要再重

复欧洲已经犯过的错误。

那么“同意”应当被如何定位，才能有利于个人信息治理体系的有效性和稳定性呢？

首先，必须承认同意作为个人信息保护合法性和正当性的基础地位，但法律也应当澄清“同意”仅可作为合法性基础之一，而不应作为数据共享的必要前提，即不能因没有获得“同意”而推断出个人信息处理行为的非法。前文已经论述，将“同意”作为必要的先决条件，可能会导致数据控制者将资源用于获得用户“同意”而非切实增强个人信息保护上。所以，如果法律文本能够明确规定：没有得到同意不等于违法，而只是需要其他证据证明合法性，则可大大缓解这种资源错配的情况。而从现在的立法情况来看，“同意”仍然是默认的必要条件，只是在这个默认条件的前提下，还存在一些“例外”。

第二，是否获得个人数据主体的“同意”可以作为判断恶意或者过错的因素之一，但不能简单地以同意原则作为任何情况下不当收集个人信息的合格抗辩[9]。也就是说，当个人数据主体与数据控制者产生争议，需要判断数据控制者是否违反了法律的规定、违背了双方的用户协议、或者是否侵犯了民法意义上的隐私权时，如果数据控制者能够出具证明其索取并获得了个人数据主体的“同意”，这一“同意”可以被作为判断责任的因素之一。但数据控制者所获得“同意”的记录并非不是绝对的免责条件，司法机关还需要分析获得这种同意的过程是否合理和正当，同时，即使没有这种同意的记录，数据控制者也可以用其他证据(例如类似 GDPR 第 6 条中、同意条款之外的其他情形)来证明自己行为的正当性。

第三，在数据处理的利益相关人对利益分配产生纠纷，而需对民事责任进行判断的情况下，应当回归到既有的民事法律逻辑的概念体系中(例如侵权法或合同法)去寻找解决方案，以“是否体现了个人数据主体真实的意思表示”(加入原告诉求是基于合同)或者“是否存在过错”(假如原告诉求是基于侵犯人格权)作为判断数据处理行为合法性的原则。

5. 结论

目前，世界上比较成熟的数据保护法规(例如 GDPR)都含有数据处理的多重正当性的规定，承认包括数据控制者的合法利益、为履行法律义务所必须的处理，以及公共利益在内的其他理由也是合法处理个人信息的前提。这实际上是力图限制过度依赖“同意”给个人信息保护体制带来的弊端，而使用通过其他因素来平衡数据控制者与个人数据主体对个人信息处理过程中的利益。从这个角度看，一些亚洲国家的立法(如菲律宾、中国内地)中，似乎忽视了这样一个这个背景，仍然或明或暗地将“同意”作为数据处理的根本前提或者首要的合法性基础。

以《草案》中以“同意”为前提，以其他为例外的立法逻辑为例，将其他多重正当性的规定作为同意制度例外规则的立法逻辑应当被予以反思，同意的例外虽然在一定程度上平衡了同意机制与其他合法利益，看似是对同意机制的地位做出的新调整，但仍然不足以扭转同意为核心的体系。因此，笔者认为，我国在针对个人信息保护相关法律在未来的修订中，可能需要跳出同意原则的框架，同意可以作为考察个人信息共享行为正当性的若干因素之一，但不应被作为逻辑上的必要前提。具体包括如下两个方面：

1) 法律文本能够明确规定：没有得到同意的个人信息处理行为不等于非法行为，而只是需要其他证据证明合法性。

2) 在制定民事责任的判断标准时，应当回归传统民法的分析框架中——从侵权法的角度分析个人信息处理行为是否存在过错，以及这种过错与损害后果之间是否存在因果关系。即使数据控制者能够提供数据主体同意的记录，也不必然被免除责任。如果原告能够证明其受到损害并且损害后果与数据处理行为存在侵权法上的因果关系，则被告也应当承担责任。此外，除了获取数据主体的同意之外，还需重点规范数据控制者应当做哪些工作让其个人信息处理获得合法性，而不是把执法者和行政相对人的精力和资源过度消耗在“同意”的形式上。

参考文献

[1] Fred, H. (2006) Personal Information in Government Records: Protecting the Public Interest in Privacy. *Saint Louis University Public Law Review*, **25**, 63-122.

[2] 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.

[3] Carolan, E. (2016) The Continuing Problems with Online Consent under the EU’s Emerging Data Protect Ion Principles, *Computer Law & Security Review*, **32**, 462-463. https://doi.org/10.1016/j.clsr.2016.02.004

[4] Solove, D. (2013) Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, **6**, 1880-1903.

[5] Crawford, K. and Schultz, J. (2014) Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review*, **55**, 93-128.

[6] Cohen, J.E. (2001) Privacy, Ideology, and Technology: A Response to Jeffrey Rosen. *Georgetown Law Journal*, **89**, 2029-2043.

[7] 高富平. 个人信息使用的合法性基础——数据上利益分析视角[J]. 比较法研究, 2019(2): 72-85.

[8] Schwartz, P.M. and Peifer, K.-N. (2017) Transatlantic Data Privacy. *Georgetown Law Journal*, **129**, 115-179.

[9] 张新宝. 个人信息收集: 告知同意原则适用的限制[J]. 比较法研究, 2019(6): 1-20.