财经法学 No. 1，2022
pp. 3 - 17

信息主体同意的适用边界

李群涛　高富平*

内容提要：在欠缺其他合法性基础情形下，信息主体同意是否适用，关键在于处理的个人信息是否含直接标识符。直接标识符能单独表征信息主体身份，从而使信息处理风险与信息主体身份精准连结。因此，出于尊重陌生人社会信息主体隐匿身份的自由、尊重信息主体对处理风险的自主决策，信息主体可以通过同意控制含直接标识符的个人信息，即“单独识别个人信息”。但同意不适用于“结合识别个人信息”。首先，结合识别个人信息具有模糊性，个人信息处理者难以就此直接识别信息主体身份进而征求同意。其次，《个人信息保护法》确立了处理结合识别个人信息不需告知规则，逻辑上也要求有相应的不需同意规则。最后，结合识别个人信息不适用同意规则也是实现“促进个人信息合理利用”这一立法目的的可行路径。

关键词：单独识别个人信息　结合识别个人信息　同意　直接标识符　个人信息保护法

一、引　言

《民法典》与《个人信息保护法》已经相继出台，作为个人信息保护制度重要内容的同意规则，其框架已经建构完成。无论《民法典》第1035条第1款第1项还是《个人信息保护法》第13条第1款第1项，都确认“信息主体同意”这一合法性基础的重要地位。然而在解释上尚未明确之问题为：当不具备《个人信息保护法》第13条第1款第2至7项所列举的合法性基础时，[1]信息主体同意是否适用于对各类个人信息的处理行为。此即本文尝试回答的信息主体同意之适用边界问题。

针对信息主体同意之适用边界问题，学界已有讨论，并形成四种学说。按照各学说主张的适

* 李群涛，华东政法大学法律学院博士研究生；高富平，华东政法大学法律学院教授。

〔1〕 关于《个人信息保护法》第13条所列七项合法性基础的研究，参见程啸、王苑：《论个人信息处理中无需取得个人同意的情形》，载《人民司法》2021年第22期。

用范围从小到大排列，分别为“无适用空间说”“敏感个人信息说”“全部个人信息说”和“全部个人信息＋匿名信息说”。笔者逐一简要述评。

“无适用空间说”认为，同意规则不能适用于任何个人信息之上，甚至不宜作为个人信息处理的合法性基础。〔2〕然而，《民法典》和《个人信息保护法》仍然坚守同意规则，故该说不为现行法所接纳。

“敏感个人信息说”认为，同意规则仅适用于敏感个人信息。〔3〕然而目前同意规则位于《个人信息保护法》“个人信息处理规则”章的“一般规定”中，该制度的体系位置至少表明一般个人信息并非一概不适用同意规则。故该说亦不为现行法所接纳。

“全部个人信息说”认为，同意规则适用于全部个人信息。〔4〕当然该说亦承认应当针对不同类别个人信息建构一套宽严有别的梯度保护体系。〔5〕该说似符合法条文义，但不利于实现《个人信息保护法》所确立的“促进个人信息合理利用”的立法目的。笔者将于本文第三、四部分详细论证，此处不赘。

“全部个人信息＋匿名信息说”认为，同意规则适用于现行《个人信息保护法》中规定的个人信息与匿名信息。〔6〕然而无论《网络安全法》第 42 条第 1 款但书，还是《民法典》第 1038 条第 1 款但书，抑或《个人信息保护法》第 4 条第 1 款皆明定匿名信息不适用同意规则。因此，该说亦不为现行法所采。

综上，关于信息主体同意的适用边界问题，上述四说均难谓妥当。

个人信息是与个人有关的各种信息，同意是个人信息处理的合法性基础，个人信息处理者为取得同意，在收集个人信息之前即需判断信息主体身份。然而个人信息范围无边无界，大量个人信息在信息主体身份判断方面具有模糊性，这对个人信息处理者于处理前履行“取得同意义务”造成障碍。

于是，本文提出，按照是否含直接标识符的标准将个人信息划分为“单独识别个人信息”与“结合识别个人信息”，同意规则仅适用于单独识别个人信息。事实上此种对个人信息的分类方法在学界的讨论中并不少见，〔7〕甚至已经为现行法所接纳（《民法典》第 1034 条第 2 款），但是鲜有观点将此种分类与同意规则的适用边界相联系并进行证成。〔8〕本文首先勾勒该边界的轮廓，

〔2〕 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。

〔3〕 参见汤敏：《论同意在个人信息处理中的作用——基于个人敏感信息和个人一般信息二维视角》，载《天府新论》2018 年第 2 期。

〔4〕 参见陆青：《个人信息保护中“同意”规则的规范构造》，载《武汉大学学报（哲学社会科学版）》2019 年第 5 期；徐丽枝：《个人信息处理中同意原则适用的困境与破解思路》，载《图书情报知识》2017 年第 1 期。

〔5〕 参见丁晓强：《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》，载《法学评论》2020 年第 4 期。

〔6〕 参见林洹民：《个人信息保护中知情同意原则的困境与出路》，载《北京航空航天大学学报（社会科学版）》2018 年第 3 期。有必要指出，该说否认存在匿名信息，因为技术界人士已经明确表示不存在绝对不可复原的匿名信息。在此基础上，按照该说，仅当法律规定了不准复原义务时，现行法所述的匿名信息才豁免适用同意规则。

〔7〕 参见陶盈：《我国网络信息化进程中新型个人信息的合理利用与法律规制》，载《山东大学学报（哲学社会科学版）》2016 年第 2 期。

〔8〕 有学者曾提及此方面，但并未展开。参见胡文华、黄道丽、孔华锋：《个人数据保护“同意规则”的检视及修正》，载《计算机应用与软件》2018 年第 9 期。

进而分别论证同意适用于单独识别个人信息，而不适用于结合识别个人信息。

二、信息主体同意规则适用的判断标准：含直接标识符

信息主体同意是否适用，其判断标准就在于个人信息是否含有直接标识符。在重视和重新界定直接标识符概念的基础上，个人信息分为单独识别个人信息与结合识别个人信息。

（一）直接标识符概念的重视与重新界定

直接标识符是指能够单独识别特定自然人身份的信息。〔9〕直接标识符的典型特征在于具有唯一性〔10〕和身份指向性，例如身份证号、社会保险号码、人脸信息等。需要注意的是，直接标识符与特定自然人是单向唯一对应关系。具言之，一直接标识符只对应唯一特定自然人，但一特定自然人将有许多直接标识符。所谓身份指向性意味着存在直接标识符即足以识别信息主体真实身份。正如学者所言，信息的人格属性集中体现在其可识别特定自然人身份的性质。〔11〕

我国立法已经接纳了直接标识符概念。我国个人信息概念借鉴欧美，而这一来源于欧美的概念恰恰无法脱离直接标识符。例如，欧盟《一般数据保护条例》（GDPR）第 4 条 a 项后半句中的身份证号等系本文所述直接标识符。同样地，美国立法一直强调直接识别符（direct-identifier）概念作为个人可识别信息（PII）的重要判断标准。与这一国际趋势相一致，我国实质上已经接受直接标识符概念，《网络安全法》第 76 条第 5 项以及《民法典》第 1034 条第 2 款，都具体列举了不少直接标识符，如身份证号码、生物识别信息等。

直接标识符可谓信息主体风险的重要来源。现代社会是风险社会，技术应用确实会给人类带来一定风险。同样地，在个人信息领域，大数据技术应用可能导致风险产生。然而，如果风险产生无法对应特定身份、不会影响到特定自然人，那么对于该自然人而言这或许并非风险，即使是也不必过于关注和担忧。但如前所述，直接标识符的本质特征在于其唯一性和身份指向性，直接标识符恰恰使个人信息处理者可知晓特定自然人身份。直接标识符在个人信息中具有重要地位，个人信息与个人身份的勾连往往依赖直接标识符。个人信息处理风险主要在于风险能通过个人信息直接传导至具有特定身份的自然人，此中起桥梁作用者正是直接标识符。

随着时代发展，直接标识符的范围已日渐扩张。目前，直接标识符包括社会身份标识符和生物身份标识符，后者是对传统直接标识符概念的扩张。〔12〕以前，直接标识符主要指身份证号、驾照号码、护照号码、社会保险号码、军官证号、工作证号、出入证号、社保卡号、居住证号码等社会身份标识符。〔13〕生物身份标识符后来也成为直接标识符的重要来源。例如，随着人脸识别技术发展，人脸信息等与特定信息主体之间也形成了唯一对应和身份指向关系。总之，某符号

〔9〕 参见《中国互联网定向广告用户信息保护行业框架标准》。

〔10〕 参见范姜真媺：《大数据时代下个人资料范围之再检讨——以日本为借镜》，载《东吴法律学报》2017 年第 2 期。

〔11〕 参见刘士国：《信息控制权法理与我国个人信息保护立法》，载《政法论坛》2021 年第 6 期。

〔12〕 参见《信息安全技术个人信息安全规范》（GB/T 35273—2020），附录 A，第 23 页；上海市地方标准《数据去标识化共享指南》（DB31/T 1311—2021）。

〔13〕 参见《信息安全技术个人信息安全规范》（GB/T 35273—2020）之附录。

具有唯一性和身份指向性，即可被认定为直接标识符。

直接标识符与间接标识符、准标识符均非同一概念。一方面，直接标识符与间接标识符并非同一概念。如果仅就“唯一性”而言，手机等智能设备序列号（又称“国际移动设备识别码”，简称 IMEI）也具有唯一性。仅依此虽能触及个人但不能识别个人身份，因此不具有前述直接标识符的“身份指向性”特征。于是，本文称之为“间接标识符”。另一方面，直接标识符与准标识符亦非同一概念，两者差异为是否具有唯一性。美欧都有实质意义上的准标识符概念。美国的准标识符（quasi-identifier）〔14〕对应欧盟 GDPR 第 4 条 a 项中的“个人属性”（factors），包括民族、种族、婚姻状况、身体、心理、基因、精神状态、经济、文化、社会因素等。准标识符中的“准”（quasi）字表明其本质上并非标识符。一个准标识符可能会对应多位自然人，不具有唯一性。例如，“研究生”是准标识符，能够对应千千万万研究生，无法指向特定自然人身份。

（二）基于直接标识符对个人信息的区分

以是否含有直接标识符为标准可将个人信息周延地分为单独识别个人信息和结合识别个人信息。

1. 单独识别个人信息

以前对个人信息相当部分的讨论恰以单独识别个人信息为基本思考模型。事实上 20 世纪即已经产生个人信息保护问题，当时个人信息即以单独识别个人信息为主。例如：“姓名张三，性别男，年龄 65 岁，身份证号 123456789012345678，电话号码 12345678901，家庭住址青海省西宁市湟源县胜利镇未来街道幸福小区 1 栋 1 单元 1025 号，银行卡号……”此为含有直接标识符个人信息（即单独识别个人信息）的典型样态。个人信息处理者据此能直接了解此个人信息对应的信息主体身份。单独识别个人信息的典型特征即在于含直接标识符。就此而言，《民法典》第 1034 条第 2 款中的“能够单独识别特定自然人的信息”与《个人信息保护法》第 4 条第 1 款中的“与已识别的自然人有关的各种信息”可表达同一含义。正因如此，本文一律用“单独识别个人信息”指代含直接标识符的个人信息。

单独识别个人信息，强调信息“含”直接标识符，而非除直接标识符之外没有其他信息。换言之，一旦数据集中含有直接标识符，直接标识符与其后跟随的购物记录、行踪轨迹等结合组成单独识别个人信息。如上所述，随着时代发展，直接标识符的概念有所扩张，生物身份标识符即为直接标识符的最新内容。因此，单独识别个人信息之范围亦相应扩张，兹不赘述。另外，是否“含”直接标识符，应当以数据集为单位全面审视，而非割裂个别数据项而单独看待。就此而言，直接标识符有可能是由一个数据集中多个数据项共同组成的，例如，在一个含有姓名、性别、学校、班级、行踪轨迹等数据项的数据集中，姓名、性别、学校、班级将共同构成直接标识符。

〔14〕 也有译为“间接标识符”，但须指出，此间接标识符与本文所谓间接标识符并非同一含义。参见刘颖、谷佳琪：《个人信息去身份化及其制度构建》，载《学术研究》2020 年第 12 期；程海玲：《个人信息匿名化处理法律标准探究》，载《科技与法律》2021 年第 3 期。

2. 结合识别个人信息

与单独识别个人信息相对的是结合识别个人信息，即不含直接标识符的个人信息。《民法典》第1034条第2款中“能够与其他信息结合识别特定自然人的各种信息”以及《个人信息保护法》第4条第1款中“与可识别的自然人有关的各种信息”，描述的均为不含直接标识符的个人信息。为表统一，本文一律用“结合识别个人信息”的概念。

结合识别个人信息也属于个人信息的范畴，但在未与直接标识符相结合的情况下，仅凭结合识别个人信息难以识别身份。换言之，信息主体以外的人仅通过结合识别个人信息来识别个人身份是需要成本的。目前个人信息定义无限扩张，这几乎成为国际社会的共识。欧盟第29条工作组出台的关于个人信息概念的意见对个人信息概念明显采广义理解，强调与其他信息结合能识别自然人身份或者特征，以及综合考虑内容、目的和影响三因素的情况下与个人有关系。〔15〕甚至按照欧洲学者分析，天气信息有时也能成为个人信息。〔16〕经扩张后的个人信息概念，其判断标准已经从能识别身份变为相关处理行为对人（不一定为特定自然人）有风险的信息。〔17〕按照《个人信息保护法》第4条第1款对个人信息的定义，我国接受了此种扩张标准。此标准非以信息当下状态为观察视角，而是要求立足当下预测充满无限可能之未来，即以未来看现在，这使得个人信息边界显著扩张且趋于模糊。从此角度而言，信息即使不含直接标识符，亦不妨碍被认定为个人信息从而适用个人信息保护相关规则。

结合识别个人信息大致有两类来源：一是各类传感器设备所收集的个人信息；二是从原始处理者或其他处理者处间接获取的经去标识化处理的信息。一方面，随着传感器的广泛布设，智能穿戴设备、网络设备的普及以及物联网技术的飞速发展与充分应用，海量的个人相关信息被快速采集供给、实时加工分析。但是相应地，部分传感器等设备能做到的只是实时记录个人有关情况而无法提供个人直接标识符等信息（信息主体主动提供的除外）。另一方面，随着信息实践不断开展，部分主体所控制的信息已经是经去标识化处理的信息。

需要注意结合识别个人信息与匿名信息的关系。所谓匿名信息是指经处理无法识别个人且不能复原的信息（《个人信息保护法》第73条第4项）。匿名信息制度通行于欧美而非我国独创。欧盟GDPR“鉴于条款”（recital）第26段明确指出，匿名信息（anonymous information）不适用于该法。该段同时指出，为了确定自然人是否可识别，应当考虑个人信息处理者或其他人（by another person）的识别能力，因此，匿名信息意味着任何人都无法通过匿名信息识别自然人身份。简言之，欧盟规定的匿名信息客观上不具有识别可能性。不过有专家已经声明，技术方面“匿名化是一种幻想”，只能达到识别可能性比较低的水平。〔18〕美国法学会2020年公布《数据隐私法律原则重述》，并在第2条中指出，无法识别个人的（non-identifiable）信息不适用数据隐私

〔15〕 See Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data, 01248/07/EN WP 136.

〔16〕 See Nadezhda Purtova, The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law, 10 *Law, Innovation and Technology*, 40 (2018).

〔17〕 参见范为：《大数据时代个人信息保护的路径重构》，载《环球法律评论》2016年第5期。

〔18〕 See Ohm, Paul, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 *UCLA Law Review*, 1701 (2010). 当然，由此观之欧盟规定的匿名信息认定标准并不合理，对此本文不再详述。

保护原则。〔19〕不同的是，欧盟匿名信息指客观上无识别可能性，而美国“无法识别的个人信息”是指识别可能性极低。然而此种无法识别的个人信息仍具有一定的识别可能性，如果不使其受制于个人信息保护规范，那么将使该部分信息暴露于风险之中。为了弥补这一点，美国的匿名信息制度有其预设前提，即禁止再识别。〔20〕或许是受欧美影响，我国《个人信息保护法》第 4 条第 1 款规定匿名信息不属于个人信息。然而借鉴比较法的重要前提是我国与借鉴对象有相同的制度环境。〔21〕我国《个人信息保护法》第 73 条第 4 项没有明确规定禁止再识别要求，且在难存此解释空间的情况下，一旦将我国匿名信息等同于美国无法识别的个人信息，将导致对匿名信息的处理失去控制。而且从笔者梳理的 50 多个法域的法律文本来看，极少有对个人信息定义作如此限制的先例。但《个人信息保护法》既已作如此规定，只能认为应对匿名信息进行严格把握，当无法确定是否满足客观“不能复原”要件时，应当认定该信息为结合识别个人信息而非匿名信息。

三、同意规则适用于单独识别个人信息

信息主体能够以同意来控制个人信息的处理行为，其正当性基础在于由宪法上的个人尊严、自由以及主体地位推演而得的个人事务自决。〔22〕笔者以下欲指出，在个人信息领域，个人事务自决主要体现为尊重陌生人社会个人隐匿身份的选择和自由，以及尊重信息主体对处理风险的决策。此二理由均仅指向单独识别个人信息。

（一）尊重陌生人社会个人隐匿身份的自由

现代社会是陌生人社会，〔23〕隐匿身份是陌生人社会中的个人选择和自由。〔24〕人口增加、人口流动性增大和社会不安全因素混杂，导致公众轻易不愿意暴露身份。虽然社会交往要求社会中每个人必须允许其他人了解自己，但是此种要求也应仅限于与个人有交往关系之人。例如，一个人的亲朋好友、同事、老师、同学、交易对手，甚至欲与其缔结合同者。但不应无限扩展到千里之外与个人毫无瓜葛的陌生人。逐渐地，是否隐匿身份成为个人自主决定的事项，受到社会认可和法律保护。

---

〔19〕 See The American Law Institute, Principles of the law-Data Privacy (2020), available at https://1.next.westlaw.com/Document/I0f02ee65145811eb8a02f30620293de0/View/FullText.html?ppcid=1c4fd268d6b54fc98b7f1ebff22c23f3&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=%28sc.Search%29, last visited on Dec. 3. 2021.

〔20〕 按照美国《数据隐私法律原则重述》(2020) 的总结，其所谓不适用数据隐私法律原则的匿名信息条件有三：第一，采用合理方法去掉个人信息上的标识符；第二，使去标识符后的个人数据处于较低风险水平；第三，个人信息处理者不再重新识别个人。

〔21〕 参见〔德〕茨威格特、克茨：《比较法总论》(上)，潘汉典等译，中国法制出版社 2014 年版，第 30 页。

〔22〕 参见田野：《大数据时代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；王雪乔：《论欧盟 GDPR 中个人数据保护与“同意”细分》，载《政法论丛》2019 年第 4 期；高富平：《同意≠授权——个人信息处理的核心问题辨析》，载《探索与争鸣》2021 年第 4 期。

〔23〕 近年来已经有相关文件关注到陌生人社会这一社会转型现象。参见《东莞市人民政府办公室关于印发〈东莞市深化“二标四实”工作总体方案〉的通知》(东府办〔2018〕44 号)；《江苏省民政厅对省十三届人大一次会议第 5015 号建议的答复》。学理上的讨论，参见张清、王露：《陌生人社会与法治构建论略》，载《法商研究》2008 年第 5 期；龚长宇、郑杭生：《陌生人社会秩序的价值基础》，载《科学社会主义》2011 年第 1 期；何绍辉：《论陌生人社会的治理：中国经验的表达》，载《求索》2012 年第 12 期。

〔24〕 参见龚长宇：《陌生人社会：价值基础与社会治理》，中国人民大学出版社 2021 年版，第 105 页。

然而，处理单独识别个人信息，将侵犯个人自主决定是否隐匿身份的自由。单独识别个人信息处理强调获得个人同意，其背后价值观与陌生人社会伦理基础不可分割。有学者称，“个体对于个人隐私和个人信息的身份识别的保护就是基于传统熟人环境社会下的潜在人格尊严和人格自由意识，而人们对于识别性的风险和恐惧多来自于传统观念下的身份泄露”〔25〕。显然，这种保护身份意识蔓延到了陌生人社会，成为个人典型的自由。如果毫不相干的主体欲全面了解一陌生人的单独识别个人信息（事实上就是了解身份），那么实在无任何正当性可言。虽然许多学者提及将分散的个人信息汇聚成大数据对于发挥数据经济价值、促进公共福利具有重大意义，但是直接标识符并非达致该目标所利用的大数据之必需。难以想象无任何交往关系的陌生私主体为了促进公共利益，需要利用他人之个人信息而且非含直接标识符不可。笔者强调，本文讨论的前提是不存在《个人信息保护法》第 13 条第 1 款第 2—7 项合法性基础，故为紧急救助而处理个人信息的情形不在本文讨论范围。正因如此，有学者指出，二次利用个人信息的首要条件是脱敏，即除去直接标识符。〔26〕简言之，陌生人可以收集他人的个人信息甚至进行个性特征分析，但是不允许其擅自知晓该“他人”的真实身份。社会学学者将这种秩序称为对陌生人“冷漠的尊重”。〔27〕

只有获得特定信息主体同意，才能使个人信息处理者与特定信息主体之间的显名交往正当化。在陌生人社会中，应然社会秩序是尊重他人的不同观念和不同选择。每个人相对于他人皆为“道德异乡人”，抱有不同信念、恪守不同行为规范；仅当取得他人“允许”“同意”“包容”时才能达成双方间新的共同行为规范。〔28〕陌生人社会的价值观在于每个人仅允许与其有关系的人了解其个人身份（当然随着关系远近了解程度会有不同），没有社会关系的陌生人不能了解其个人身份。与此相对应，允许与特定个人没有社会关系的人收集、使用该特定个人的个人信息，但仅限于收集、使用结合识别个人信息且不得在分析特征的过程中分析出真实身份。这便是个人信息领域陌生人的行为规范。如果处理单独识别个人信息，则等同于突破陌生人之间行为规范，因此，只有获得信息主体的同意以形成双方间新共同行为规范时，处理单独识别个人信息才被允许。或许出于类似考虑，有学者也指出信息主体能够支配自己的姓名、身份证号码、相貌特征等等。〔29〕此观点值得赞同。

（二）尊重信息主体对处理风险的决策

直接标识符的存在使得信息处理风险得以精准传导至具有特定身份的自然人。“风险可以被界定为系统地处理现代化自身引致的危险和不安全感的方式。”〔30〕如直接标识符定义所阐释，其最大特征为与特定自然人身份具有唯一对应性。个人信息处理者通过其所控制的单独识别个人信

〔25〕 苏今：《〈民法总则〉中个人信息的“可识别性”特征及其规范路径》，载《大连理工大学学报（社会科学版）》2020 年第 1 期，第 86 页。

〔26〕 参见姬蕾蕾：《论个人信息利用中同意要件的规范重塑》，载《图书馆》2018 年第 12 期。

〔27〕 参见前引〔24〕，龚长宇书，第 19 页。

〔28〕 参见前引〔24〕，龚长宇书，第 115－116 页。

〔29〕 参见郭明龙：《论个人信息之商品化》，载《法学论坛》2012 年第 6 期；韩强：《人格权确认与构造的法律依据》，载《中国法学》2015 年第 3 期。

〔30〕〔德〕乌尔里希·贝克：《风险社会》，何博闻译，译林出版社 2004 年版，第 19 页。

息便能直接识别信息主体而不需要进行任何处理行为（识别行为）。对此类单独识别个人信息进行分析，其决策结果可以通过直接标识符的桥梁作用精准配置于特定自然人。此种结果对于特定自然人而言可能有好有坏。例如，银行处理特定自然人单独识别个人信息用以评估该特定自然人信用情况，当处理结果符合信用要求时对该自然人而言有正向反馈，但当处理结果不符合信贷政策所要求的信用等级时，对于该自然人而言具有不利影响，因为这将关系到信息主体是否能顺利申请贷款。但算法不同以及其他因素，导致处理分析行为结果是好是坏无确定性甚至不可预期，这本身对于信息主体而言即为一种风险。除此之外，此类个人信息的滥用以及被篡改、毁损、丢失等都是对信息主体的风险。从《居民身份证法》《统计法》《刑法》等条文来看，我国个人信息立法的重要目的恰是为维护自然人人身、财产安全免受威胁。〔31〕

既然直接标识符的存在客观上产生了个人信息处理的风险与信息主体身份连结的效果，那么出于个人事务自决，应当允许个人对其未来风险进行自主判断和决定。尤其是当个人信息处理者从信息主体处直接收集个人信息时，双方处于直接交互状态，同意机制落实也较为简单。〔32〕如果立法者倾向于剥夺个人判断决策资格而一律允许个人信息处理者处理此类个人信息，那么即剥夺了个人自主决定、自主判断空间，此为典型的法律父爱主义，〔33〕将使信息主体暴露于个人信息处理的风险之中。即使法律对个人信息处理者行为进行规范和要求，也不能保证个人信息处理者必然严格遵守规则，此即禁止性规定会配套法律责任条款的重要原因。不仅如此，即便个人信息处理者遵守各类规定，也不见得处理行为不产生任何风险。当然，允许信息主体自行决策，原理在于允许个人对于精准连结身份的未来风险进行判断和决策，而非出于个人对其个人信息的完全控制。〔34〕关于该点，有学者通过细致考究已经指出，目前广为流传的个人信息自决权是对德国人口普查案的以讹传讹，〔35〕所以此处信息主体同意是个人自治的具体体现，是个人事务自决的应有之义。

事实上，避免存在直接标识符而导致信息处理风险精准传导至个人，亦符合国际个人信息保护制度的基本逻辑。以下以具有代表性的美国和欧盟的制度分别说明。

美国的信息主体同意规则重点关注可识别个人信息（personally identifiable information，简称 PII），即本文所述单独识别个人信息。起初按照美国的隐私控制理论，信息主体有资格决定个人信息在何时、以何种程度和方式进行流动。〔36〕但是隐私控制理论与美国人的信息自由信仰背道而驰。此种情况下，为了缓和信息控制和流动之间的张力，美国通过《儿童网络隐私法》等一系列法案将信息主体对个人信息的控制限制在 PII 范围内，即处理 PII 要经过信息主体同意，而 PII 恰恰相当于本文的单独识别个人信息。虽然美国分散式个人信息保护立法使 PII 的边界动态变化，但美国人的信息主体仅控制 PII 的立场却始终坚定。甚至根据美国最新出台的《统一个人

〔31〕 参见高富平：《个人信息保护立法研究》，光明日报出版社 2021 年版，第 195 页。

〔32〕 参见前引〔8〕，胡文华等文。

〔33〕 参见孙笑侠、郭春镇：《法律父爱主义在中国的适用》，载《中国社会科学》2006 年第 1 期。

〔34〕 关于该问题的讨论，参见前引〔22〕，王雪乔文；张勇：《APP 个人信息的刑法保护：以知情同意为视角》，载《法学》2020 年第 8 期；前引〔11〕，刘士国文。

〔35〕 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。

〔36〕 See Alan F. Westin，Privacy and Freedom，25 *Washington and Lee Law Review*，166（1968）.

数据保护法》（The Uniform Personal Data Protection Act，简称 UPDPA）〔37〕第 7 条第 b 款第 5 项结合同条第 a 款第 1 句，可以得出结论：针对去直接标识符的个人信息进行处理不需要获得信息主体的同意。〔38〕例如，在针对群体的医学研究中，为了研究某种疾病的地域分布关系，在收集各地患者数据时，至多同时收集患者所在省、市、县即可，没有必要得知患者姓名、身份证号等数据项，甚至患者的精确地址亦不具有必要性。此时个人信息处理者便不需要取得信息主体的同意。由是观之，美国人基本认为若无 PII 则不存在权益威胁。

欧盟的制度也体现了类似的思路。欧盟 2016 年制定了 GDPR，2018 年正式生效执行。部分关于 GDPR 的研究表明同意规则将赋予信息主体对其个人信息的超强控制力。〔39〕但在 GDPR 尚未生效执行的 2017 年，欧盟第 108 号公约协商委员会就出台了《大数据社会个人数据处理中的个人保护指南》。〔40〕其中指出，“大数据应用的复杂性和模糊性应该促使规则制定者不再将控制概念局限于个人控制（个人信息）。他们应该（将控制个人信息概念）理解为更广义的控制个人信息使用”〔41〕。显然欧盟欲澄清，信息主体同意对其个人信息的控制范围远不及研究者所言之广泛。

因此，为尊重陌生人社会个人隐匿身份的自由，尊重信息主体对处理风险的决策，信息主体同意适用于单独识别个人信息。

四、同意规则不适用于结合识别个人信息

基于尊重信息主体对处理风险的决策，以及尊重陌生人社会个人隐匿身份的自由，可以得出同意适用于单独识别个人信息的结论。基于此二者，同样能够从反面佐证同意不适用于结合识别个人信息。不仅如此，本部分另从避免《个人信息保护法》两套识别标准的“基因缺陷”、避免同意规则与不需告知规则衔接不畅，以及避免“促进个人信息合理利用”的立法目的不达三个角度证明，同意规则不适用于结合识别个人信息。

---

〔37〕《统一个人数据保护法》系由美国统一法律委员会制定，于 2021 年 7 月通过的示范法案，拟于 2022 年 1 月前后实施，该法案载于 https://uniformlaws.org/committees/community-home/librarydocuments/viewdocument?DocumentKey=afdb7812-a7c6-4468-92f6-fac09416c0ac。

〔38〕根据 UPDPA 第 7 条第 b 款第 5 项，对于创建假名或匿名化数据具有合理必要性的处理行为，是兼容的数据处理行为。根据 UPDPA 第 7 条第 a 款第 1 句，控制者或处理者可以在未经数据主体同意的情况下从事兼容的数据处理行为。因此，根据 UPDPA 第 7 条第 b 款第 5 项结合同条第 a 款第 1 句，对于创建假名或匿名化数据具有合理必要性的处理行为，不需要取得数据主体的同意。以举重以明轻的法学原理对该项规定深入研究可得出以下结论：创建假名化数据的行为针对的是能单独、直接识别数据主体的个人数据，该行为尚且不需要取得数据主体的同意，则假名化完成后的数据不能单独、直接识别数据主体，对该类数据的处理行为更不需要获得数据主体的同意。UPDPA 中的假名化数据为去除直接标识符的个人数据，大致相当于本文所指“结合识别个人信息”。

〔39〕参见王成：《个人信息民法保护的模式选择》，载《中国社会科学》2019 年第 6 期。

〔40〕Guidelines on the Protection of Individuals With Regard to the Processing of Personal Data in a World of Big Data, available at https://ccdcoe.org/uploads/2019/09/CoE-170123_Guidelines-on-protection-of-individuals-with-regard-to-processing-of-personal-data-in-a-world-f-big-data.pd, last visited on Dec. 3, 2021.

〔41〕《大数据社会个人数据处理中的个人保护指南》，李群涛译，高富平校，载 http://www.dataprotection.cn/news/126.html，最后访问时间：2021 年 8 月 30 日。

（一）避免个保法两套识别标准的“基因缺陷”

认定个人信息时，采较为宽松的识别可能性标准，个人信息处理者本身是否具有直接识别能力，在所不问；然而取得同意却恰以个人信息处理者本身具有直接识别能力为前提。两者所持标准差异导致同意规则不能及于全部个人信息，特别是不适用于结合识别个人信息。〔42〕

个人信息认定环节的判断标准是客观识别标准，其要求“个人信息处理者或者其他任何人”有能力根据信息识别信息主体身份，不仅限于个人信息处理者自身有此识别能力。单独识别个人信息是个人信息中最为典型的一类。然而，随着世界各国认识到个人信息处理活动涉及信息主体利益甚巨，出于加强信息主体权益保护目的，个人信息保护法适用范围相应扩张。〔43〕作为个人信息保护法适用门槛，个人信息范围也需随之扩张。于是国际上普遍认可，若个人信息处理者不能通过信息单独识别信息主体，而是结合其他信息可以间接识别，那么该信息（结合识别个人信息）亦属于个人信息。不仅如此，在欧盟 GDPR 影响下，国际社会进一步认同：即使个人信息处理者不能通过信息识别个人，而其他任何人（by another person）具有此种识别能力，那么该信息也属于个人信息。至此，作为个人信息判断重要标准的识别，已经从特定个人信息处理者能够识别，扩张到世界上（至少是个人信息处理者活动范围内）任何其他人能够识别。此观点被欧盟第 29 条工作组严格贯彻，〔44〕欧洲法院也在相应判决中落实这一标准。〔45〕以至于欧洲学者嗟叹，个人信息保护法某种程度上已成为“万物之法”。〔46〕简言之，为了保护个人权益，已经以当前世界上先进识别技术和丰富信息量为标准（客观识别标准）判断特定信息是否为个人信息。

然而就同意规则而言，履行“取得同意”义务必然以主观识别标准——特定个人信息处理者的实际识别能力（甚至是直接识别能力）——为限。取得同意义务是个人信息处理者自身需要履行的义务，依照“法律不强人所难”的基本法理，个人信息处理者履行某义务必然要以有履行此义务的能力为限。个人信息处理者履行取得同意义务要以信息中含有直接标识符为限，此系同意的时间要求所致。按照《个人信息保护法》第 13 条第 1 款第 1 项规定，取得信息主体同意的，个人信息处理者方可处理个人信息。易言之，原则上取得同意应当先于处理行为进行方为合法。而结合其他信息进行间接身份识别也是处理行为，因此，同意也应当先于间接识别行为而进行，否则违法。同意这一时间要求，迫使个人信息处理者在取得同意之前不得以处

〔42〕 See Christopher Kuner, Lee A. Bygrave, Christopher Docksey, *The EU General Data Protection Regulation (GDPR) A Commentary*, Oxford University Press, 2020, p. 395.

〔43〕 两份个人信息保护领域的重要文件引领了对信息主体的强保护，分别是世界经济合作与发展组织发布的《隐私保护与个人数据跨境流通指南》和欧洲理事会发布的《个人数据自动化处理中的个人保护公约》。此二文件成为之后各国立法的重要参照文件。

〔44〕 参见前引〔15〕，Article 29 Data Protection Working Party 文。

〔45〕 See Case T－670/16, Digital Rights Ireland v. European Commission, GC, order of 22 November 2017 (ECLI: EU: T: 2017: 838); Case C－434/16, Peter Nowak v. Data Protection Commissioner, judgment of 20 December 2017 (ECLI: EU: C: 2017: 994); Case C－345/17, Proceedings brought by Sergejs Buivids, judgment of 14 February 2019 (ECLI: EU: C: 2019: 122); Case C－40/17, Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV., judgment of 29 July 2019 (ECLI: EU: C: 2019: 629).

〔46〕 参见前引〔16〕，Nadezhda Purtova 文，第 78 页。

理的方式进行识别。因此，同意方面的合规，要求个人信息处理者必须在取得同意之前能单独、直接识别信息主体的身份。个人信息认定环节的客观识别标准与同意规则中的主观识别标准间的差距，使得同意控制范围注定无法及于各类个人信息上的处理行为。有学者将客观标准概括为“识别可能性”（identifiability），而将主观识别标准概括为“识别本身”（identification），并指出同意规则仅关注后者，即识别本身。〔47〕两种识别标准只有在面对单独识别个人信息时才重合。揣测普遍漠视这一差距的原因，或许是个人信息保护制度研究基本以 APP 从信息主体处直接采集个人信息的场景作为典型思考模型。于是，收集、存储、分析个人信息，当然不存在不知信息主体身份的情形。此亦从侧面说明，同意规则适用范围的限缩，往往起因于个人信息处理者非从信息主体处直接收集个人信息情形（即俗称的“个人信息二手利用”）的广泛存在。总之，个人信息的外延比同意规则所能适用的个人信息外延大得多，超出的部分包括特定个人信息处理者能够结合识别出身份的个人信息以及特定个人信息处理者本身不能结合识别出身份的个人信息。

两标准范围的不完全重合，恰恰是由于个人信息认定环节“识别”标准的极大扩张为个人信息保护制度创设的“基因缺陷”。由此观之，对个人信息范围采广义理解的国家，只要其采选进机制（opt-in），即取得同意应先于处理行为进行，则其个人信息保护体系中的同意规则亦需限缩于单独识别个人信息。欧盟发现了这一基因缺陷，并通过设置 GDPR 第 11 条试图进行解决。根据该条，个人信息处理者〔48〕有时不必仅为了合规而获取信息主体同意。也正因如此，欧洲学者赞扬 GDPR 第 11 条称，该条“弥合了（至少是试图弥合）由个人信息概念引发的鸿沟”〔49〕。

（二）避免同意规则与不需告知规则衔接不畅

同意不适用于结合识别个人信息，即要求针对结合识别个人信息建立“不需同意”制度。此系对《个人信息保护法》“不需告知”制度的必要呼应。

《个人信息保护法》设立了不需告知规则。《个人信息保护法》第 18 条第 1 款为“不需告知”制度提供了依据。“不需告知”制度主要适用于三种情形：第一，信息主体已经知情，不再需要告知；第二，已经公开的个人信息，不再需要告知；〔50〕第三，当个人信息处理者客观不识别身份或基于合规要求不被允许识别身份时，基于法律不强人所难的基本法理，也应当作为前述不需要告知情形之一。GDPR 有类似制度，其第 13、14 条分别针对从信息主体处收集个人信息、非从信息主体处收集个人信息两种情形规定了告知义务的例外情形。尤其是第 14 条第 5 款 b 项提出，个人信息处理者提供相应信息被证明是不可能或者需要投入过多不必要精力时，个人信息处理者不需要告知。不过，GDPR 亦非完美：根据 GDPR 第 11 条第 2 款，当个人信息处理者的处

〔47〕 参见前引〔42〕，Christopher Kuner 等书，第 395 页。

〔48〕 GDPR 与我国《个人信息保护法》在术语使用上略有不同。GDPR 的数据控制者对应我国的个人信息处理者。GDPR 的数据主体，对应我国的个人，即本文所谓信息主体。术语上的不统一将导致文本阅读上的障碍，为避免这一问题，本文在介绍 GDPR 条文时一律使用我国的术语。

〔49〕 前引〔42〕，Christopher Kuner 等书，第 395 页。

〔50〕 参见程啸：《论个人信息处理者的告知义务》，载《上海政法学院学报（法治论丛）》2021 年第 5 期。

理目的不要求识别信息主体身份，且个人信息处理者能够证明自己无法识别信息主体时，如果个人信息处理者可以（if possible），则需要履行告知义务。然而当个人信息处理者不能识别信息主体时，个人信息处理者如何能够履行告知义务。于是，欧洲学者亦无奈表示，只能依赖“如果可能的话”（if possible）这一条件弥补第 11 条第 2 款的缺憾。〔51〕换言之，一般宜认为此种情况下告知义务无履行可能。

因为告知是取得同意的前提和要求，所以不需告知规则应配以不需同意制度。按照《个人信息保护法》第 14 条第 1 款第 1 句，同意应当在信息主体充分知情的前提下作出。但当信息主体不知情时（此为常态），个人信息处理者必然需通过告知使其充分知情。是故，在逻辑上告知、知情、同意依次发生，通常情况下告知是同意的逻辑前提。“告知同意”或者“知情同意”这一学界和实务界通用且公认的提法事实上已经表明告知是同意的逻辑前提。〔52〕既然如此，那么由于客观或者合规等原因不能告知信息主体时，当然也就无法取得信息主体的同意。这就要求《个人信息保护法》有对应不需告知规则的不需同意制度。

然而《个人信息保护法》没有同步设计不需同意制度。我国虽然设计了不需告知规则，但显然同意规则与此不相适应，因为按照第 13 条规定的文义，当无其他合法性基础时，各类个人信息的处理都需要以获得信息主体同意为前提，其他因素在所不问（此亦为本文引言中“全部个人信息说”的依据）。从全国人大相关机构在立法过程中形成的一系列有关欧盟个人信息保护制度和美国隐私保护制度的研究材料，以及《个人信息保护法》众多条文的表述观之，我国《个人信息保护法》立法明显有参考 GDPR 的现象。然而仅就告知同意规则来看，我国并未做到全面、完整、正确地进行制度参考。上文已经提及，我国不需告知规则学习了 GDPR 第 13、14 条，但对应此种情形，GDPR 配套设置了第 11 条第 1 款不需同意规则，即如果个人信息处理者处理个人信息的目的不要求或不再要求识别信息主体身份，则不应强制个人信息处理者仅为合规而保留、获取或处理额外信息以识别信息主体身份。言下之意，当个人信息处理者不需识别身份时，其处理不需要取得同意。但是我国只吸收了不需告知规则，没有同步建立作为其逻辑后果的不需同意制度。

当然，GDPR 第 11 条第 1 款并非我国不需同意制度的最佳选择。相反，GDPR 第 11 条第 1 款本身存在严重的逻辑漏洞，此处简要分析。根据欧盟 GDPR 第 11 条第 1 款可推知，若处理之目的不要求识别信息主体身份，则以识别身份为前提的同意也不需要获得。简言之，根据该条，是否要求获得同意系以“是否需要识别身份”为根本判断标准。需要识别信息主体身份，则需要获得同意，反之则不需要。看似周延的结论掩盖了逻辑上的漏洞，此处逻辑上的漏洞主要是指遗漏考虑一种情形，即处理结合识别个人信息（即不含直接标识符的个人信息）且处理目的要求识别信息主体身份。根据 GDPR 第 11 条第 1 款，此种情形，由于“需要识别”所以需要获得同意。

〔51〕 参见前引〔42〕，Christopher Kuner 等书，第 396 页。

〔52〕 参见前引〔17〕，范为文；叶名怡：《论个人信息权的基本范畴》，载《清华法学》2018 年第 5 期；前引〔22〕，田野文；王利明：《数据共享与个人信息保护》，载《现代法学》2019 年第 1 期；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；万方：《隐私政策中的告知同意原则及其异化》，载《法律科学（西北政法大学学报）》2019 年第 2 期；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。

然而只有通过“识别身份”这一处理行为识别出信息主体身份才能得到其同意，而同意只能为同意之后的处理行为提供合法性基础，不能为同意之前的识别身份行为及其之前行为提供合法性基础。因此笔者指出的这种情况，根据GDPR第11条第1款，识别出身份之前阶段的处理行为必然将因无合法性基础而违法。法律不强人所难，所以识别身份及其之前的行为也不应当要求获得个人同意。因此，GDPR以“是否需要识别”作为划分同意适用边界的标准并不合理，应当以是否含有直接标识符（无需进行处理即可识别身份）作为划分标准。我国没有移植GDPR第11条第1款，一定意义上避免了陷入前述逻辑漏洞，但这不能表明我国不应该设立不需同意制度。

于是，我国应建立的不需同意制度，不能盲目追随GDPR，而是应基于《个人信息保护法》条文，在解释上将单独识别个人信息作为同意规则的适用范围，而将结合识别个人信息排除于同意规则适用范围之外。如前所述，我国应当存在不需同意制度。但显然，我国法缺失这一制度，导致同意规则与告知规则衔接不畅。而《个人信息保护法》生效后，必须从解释论层面寻找新出路。此即需在现行法框架下基于解释论提出具有相同功能的替代方案。而本文所提出的同意适用边界限缩恰恰是解释论下的一种有效解决方案。同意适用边界限于单独识别个人信息，并非意味着结合识别个人信息将不受控制，只是说明结合识别个人信息将不受信息主体的事前控制。但基于法律规定产生的个人信息处理者义务仍然继续适用，《个人信息保护法》规定的事前个人信息保护影响评估等措施仍然应当落实，以保护信息主体权益。并且，此时应当对个人信息处理者课以更高要求。〔53〕

（三）避免个人信息流通利用的立法目的不达

确认结合识别个人信息的处理不需要同意，恰恰能激励个人信息处理者将个人信息处理活动维持于低风险状态。个人信息保护的本意是平衡个人信息处理利用与个人信息处理利用过程中信息主体权益维护。当个人信息已经为结合识别个人信息时，已经使个人信息处理活动处于低风险水平。如果仍然认为结合识别个人信息之处理亦须取得信息主体的同意，那么必然以重新识别信息主体身份为前提，则反而因为合规要求使得个人信息重新被暴露于高风险环境。〔54〕最终与个人信息保护法立法目的相悖。正是因为单独识别个人信息与结合识别个人信息的风险水平有异，所以对两者不应采相同保护水平。结合识别个人信息之处理不需要个人同意，是对此类信息处理的制度激励，有利于鼓励个人信息处理者积极主动地对个人信息进行去标识化处理。事实上，《个人信息保护法》本身也将去标识化作为安全技术措施（第51条第3项）。

《个人信息保护法》的重要目的之一在于“促进个人信息合理利用”。信息是自由的，个人信息亦未完全脱离自由的本质，只是因为个人信息以个人为主题，所以属于特殊信息类型，需要一定程度的特殊对待。而结合识别个人信息，多属于用以分析个性特征的信息，这些信息只

〔53〕 参见前引〔42〕，Christopher Kuner等书，第447页。

〔54〕 See Paul M. Schwartz，Daniel J. Solove，The PII Problem：Privacy and a New Concept of Personally Identifiable Information，86 *New York University Law Review*，1814（2011）.

有与特定个人身份关联起来，可以直接通过该信息识别信息主体身份时，才涉及隐私等人格利益问题，这意味着鼓励在不危及信息主体权益情形下对结合识别个人信息进行分析利用。当然，若导致不利后果，那么可以通过民事侵权救济而非事前控制机制，保证信息主体权益得到保护。现行法已经建立起这样的事后救济机制。当信息主体权益遭受侵害或有受侵害之虞但尚未造成损害时，《民法典》第 1037 条等已经提供了各类防御性人格权益请求权。〔55〕当信息主体权益遭受侵害并造成损害时，《个人信息保护法》第 69 条第 1 款确立了专门的损害赔偿制度。

不过，需要强调，结合识别个人信息与单独识别个人信息可能互相转换，一旦结合识别个人信息转化为单独识别个人信息，则又需要适用同意规则。处理结合识别个人信息不必获得同意，甚至连分析行为也不必获得同意。但是一旦通过处理行为识别到信息主体身份，结合识别个人信息瞬间转换为单独识别个人信息，于是应当立即寻求信息主体的同意。此时一旦同意没有取得，那么根据《个人信息保护法》第 47 条第 1 款，个人信息处理者应当删除所涉个人信息。某种意义上，结合识别个人信息转换为单独识别个人信息的时刻，很可能是个人信息处理者删除个人信息的时刻。

五、结　语

“保护个人信息权益”与“促进个人信息合理利用”是《个人信息保护法》第 1 条确立的同等重要的立法目的。该法给法律解释适用者提出的艰巨任务是实现两个目的的和谐与平衡。然而，若认为缺失《个人信息保护法》第 13 条第 1 款第 2 至 7 项的合法性基础时，对各类个人信息的处理都要经过同意，那么天平上的砝码已经过于向保护个人信息权益一侧倾斜。划定同意规则的适用范围正是“瞻前顾后”地通盘考虑两种目标的平衡之后在同意规则上的体现。本文主张信息主体的同意只能适用于对单独识别个人信息的处理行为。此结论在法律解释上体现为应当对《民法典》第 1035 条第 1 款第 1 项主文中的“自然人”以及《个人信息保护法》第 13 条第 1 款第 1 项中“个人”概念进行限缩，限缩至“个人信息中以直接标识符直接体现其身份的个人”。当然，个人信息处理的合法性须从目的合法、具有合法性基础，以及处理行为规范三个方面综合甄别。本文讨论的同意边界问题仅是合法性基础方面判断的问题，不涉及目的是否合法和处理行为是否规范两方面。

使结合识别个人信息摆脱信息主体同意的控制，也正是在法律上为目前国家提倡的数据流通机制提供法律基础。2020 年 3 月公布的《中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见》提出加快数据要素市场建设，其内含的要求便是为数据流通创造法律上的途径。个人信息是数据中的重要类别，当然应该考虑其流通利用的合法性问题。但目前个人信息流通机制于法律方面的困境在于逐一获取信息主体的同意，合规成本极大。本文试图为结合识别个

〔55〕 参见高富平、李群涛：《个人信息主体权利的性质和行使规范——〈民法典〉第 1037 条的解释论展开》，载《上海政法学院学报（法治论丛）》2020 年第 6 期。

人信息未经信息主体同意而流通利用的可行性提供法理支撑，以便在一定程度上为个人信息的流通利用松绑。

Abstract：In the absence of other legal basis，the key to the applicability of personal information subject's consent lies in whether the personal information contains a direct identifier. The direct identifier can directly represent the identity of the personal information subject，so as to accurately link the information processing risk with the personal identity. In addition，in the stranger society，the choice and freedom of individual hiding identity should be respected. Therefore，the direct identifier representing identity information should be controlled by the personal information subject，that is，applicable boundary of personal information subject's consent is individually identifiable personal information. However，consent does not apply to personal information without direct identifier. Firstly，as the fuzziness of this kind of personal information，it is difficult for personal information processors to directly identify the subject of personal information and ask for consent. Secondly，logically，the non disclosure system established by the personal information protection law needs the non consent system. Finally，the non application of consent system is also the important way to achieve the legislative purpose of personal information circulation and utilization.

Key Words：individually identifiable personal information，personal information without direct identifier，agree，direct identifier，personal information protection law

（责任编辑：武　腾　赵建蕊）