交大法学 SJTU Law Review
No. 4 (2019)

企业数据获取“三重授权原则”反思及类型化构建

徐　伟*

目次

摘要　源于新浪微博诉脉脉案的“三重授权原则”，要求数据获取企业在获取数据持有企业的用户数据时，需满足用户对数据持有企业、用户对数据获取企业，以及数据持有企业对数据获取企业的“三重授权”。将这一原则普遍适用于所有数据类型并不妥当。企业间数据获取规则应根据数据类型的不同而作类型化构建：获取可识别的原生数据时，需获得用户同意，无须数据持有企业的同意；获取非可识别的衍生数据无需取得用户同意，但需取得企业同意；获取可识别的衍生数据需同时获得用户和企业的同意；获取非可识别的原生数据时，无须取得用户同意，是否需取得企业同意取决于数据是否公开。

关键词　企业数据权　三重授权原则　原生数据　衍生数据　不正当竞争

2019年6月举办的20国集团会议(G20)上发布了“贸易与数字经济的部长宣言”。〔1〕数字经济的重要性已成共识。与之相应，数据已成为数字经济时代的“石油”，其重要性与日俱增。正因

* 宁波大学法学院副教授、法学博士。本文系国家社会科学基金青年项目“网络服务提供者侵权责任基础理论研究”(项目编号：16CFX042)；国家社会科学重大基金项目“大数据时代个人数据保护与数据权利体系研究”(项目编号：18ZDA145)的研究成果。本文撰写受上海玛娜数据科技发展基金会“个人数据的权利结构及利益配置研究”项目资助。感谢责任编辑和外审专家的评审意见；感谢朱剑丽、孙慧芳在资料查找和整理上的协助，当然文责自负。

〔1〕 See “G20 Ministerial statement of Trade and Digital Economy” (https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf, last access 2019-07-10).

如此，企业间的数据之争正日益频繁地上演。本文试图通过对企业数据之争的判决/事件的梳理，明确企业数据之争的主要法律问题，并在此基础上提出企业数据之争的基本规则，希冀为这一目前“浑沌”的领域提供借鉴。

一、企业数据获取的典型纠纷及主要法律问题

（一）企业数据获取的典型纠纷

当前已发生的数据纠纷，主要有以下几种典型情形。

第一，数据获取企业未经用户和数据持有企业的同意而直接获取数据。〔2〕国内典型案件是2016年大众点评诉百度地图案等，〔3〕美国则有2017年的hiQ诉LinkedIn等。〔4〕在大众点评诉百度地图案中，大众点评为用户提供商户信息、消费评价（包括环境、服务、价格等，可附照片）、优惠信息等服务。百度地图不仅为用户提供导航等地图服务，也提供商户信息查询等服务。百度用户也可对商户做评价，但此类点评较少。为此，百度地图通过搜索技术获取了大众点评的用户点评数据并大量全文展示于地图软件中。大众点评主张这一行为构成不正当竞争。法院认为，百度在使用来自大众点评的评论信息时，应遵循“最少、必要”原则，即采取对大众点评损害最小的措施。百度的大量全文展示行为已超过必要限度，实质上替代了大众点评的内容提供服务，构成不正当竞争。

第二，数据获取企业获得了用户同意，但并未获得数据持有企业同意而获取数据。国内典型事件是2017年的腾讯微信与华为数据之争等。在腾讯与华为事件中，华为出品的荣耀Magic手机提供了Magic Live智慧系统，该系统可以根据微信聊天内容等自动加载地址、天气、时间等信息。比如，当用户在微信聊天过程中提及电影相关信息时，就会自动推荐近期热映大片，并根据用户的喜好提供影院与订票功能等。对此，腾讯认为，华为的上述做法实际上夺取了腾讯的数据，并侵犯了微信用户的隐私。华为则否认侵犯了用户隐私，称“任何用户信息属于用户，既不属于微信，也不属于荣耀Magic，荣耀Magic获取的信息是经用户授权并只在荣耀Magic手机上处理的，并未上传至任何云端”。并表示，荣耀Magic已通过工信部的测试，表明这款手机没有违反隐私监管规定。最终，双方间的纠纷并未形成诉讼，而是通过工信部协调解决。〔5〕

第三，数据获取企业获取数据虽获得了用户与数据持有企业的同意，但逾越了双方约定的范围而“过度”收集数据。国内的典型案件是2016年的新浪微博诉脉脉案。〔6〕在该案中，新浪微博

---

〔2〕从技术的角度而言，数据取得有抓取和获取两种，二者最大的区别在于数据方是否授权，故表述上常采“非法”抓取数据和通过接口获取数据。鉴于本文聚焦于企业数据之争，而无论抓取抑或获取都存在争议，故本文不对这两个概念做细致区分。本文的“获取”采广义理解，包括了抓取和狭义获取。

〔3〕上海汉涛信息咨询有限公司与北京百度网讯科技有限公司、上海杰图软件技术有限公司不正当竞争纠纷案，上海知识产权法院（2016）沪73民终242号民事判决书。

〔4〕See *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099 (N.D.Cal. 2017).

〔5〕参见杨鑫倢：《工信部回应华为腾讯数据之争：正组织调查，敦促企业规范搜集》，载澎湃新闻（https://www.thepaper.cn/newsDetail_forward_1756038，最后访问时间2019-08-19）。

〔6〕北京微梦创科网络技术有限公司与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不正当竞争纠纷案，北京知识产权法院（2016）京73民终588号民事判决书。同时，该案也涉及数据获取企业未经数据持有企业和用户同意而获取数据，以及违反约定使用数据的情形。

主张脉脉的下述行为不当：(1) 未经新浪授权获取微博用户的职业、教育信息。脉脉通过新浪微博提供的Open API〔7〕获取新浪微博用户的数据。根据双方间的《开发者协议》，脉脉获得的是普通级别权限，只能获得用户ID、头像等数据，无权获得用户职业、教育信息。但由于新浪微博的技术缺陷，只拥有普通级别权限的脉脉通过其获取的接口同样也获得了用户职业和教育信息。(2) 在新浪终止脉脉的API端口，终止双方合作协议后，脉脉违反《开发者协议》，仍使用之前获得的微博用户数据。(3) 未经新浪同意，绕过API获取了非脉脉用户的新浪微博数据。(4) 将获得的非脉脉用户，与脉脉用户手机通讯录中的联系人关联，导致非脉脉用户的微博信息展示在脉脉用户的脉脉软件联系人中。〔8〕法院支持了新浪微博的上述主张，认为脉脉的两项行为构成不正当竞争：一是获取、使用新浪微博用户信息的行为；二是获取、使用脉脉用户手机通讯录联系人与新浪微博用户对应关系的行为。法院的主要理由是：脉脉的信息获取、使用行为违反了双方间的《开发者协议》，未经新浪微博授权，或未经非脉脉用户同意，损害了消费者知情权等，且对公平竞争秩序构成了损害。同时，二审法院在裁判中提出企业获取数据应遵循“三重授权原则”，〔9〕即用户授权数据持有企业共享其数据，数据持有企业授权第三方企业获取其数据，用户授权第三方企业使用其数据。〔10〕

第四，数据获取企业获取数据虽获得了用户与数据持有企业的同意，但数据持有企业主张数据获取企业“不当”使用数据，比如将获得的数据再次授权给其他企业等。〔11〕国内典型案件是2019年的腾讯微信/QQ诉今日头条抖音/多闪案。〔12〕该案中，腾讯主张今日头条的下述行为构成不正当竞争并申请行为保全：(1) 在抖音产品中向抖音用户推荐好友时使用来源于微信/QQ开放平台的微信/QQ用户头像和昵称等微信/QQ数据；(2) 将微信/QQ开放平台为抖音产品提供

〔7〕 Open API(亦称API，Application Programming Interface，应用程序编程接口)，Open API意味着开放接口调取数据，实现企业间数据的共享。同时，数据提供方通过接口的权限级别，实现对第三方获取的数据范围的控制。

〔8〕 新浪微博还主张了脉脉在网络上发表的言论构成商业诋毁等，但这些主张与本文无关，故不提及。

〔9〕 本案的审判长在之后发表的文章中将“三重授权原则”的表述改为了“三重同意原则”。参见张玲玲、田芬：《涉及用户数据信息商业利用的竞争行为是否属于正当的司法判断——评上诉人淘友技术公司、淘友科技公司与被上诉人微梦公司不正当竞争纠纷案》，载《中国知识产权报》2017年4月19日，第008版。本文认为，在数据权属(尤其是企业对用户数据的权属)尚无定论的情况下，“三重同意”的表述更妥当。同时，“三重授权”是项“规则”而非“原则”。只是为尊重判决书原文和便于与目前学界相关研究对话，会在行文中根据语境使用“授权”/“同意”“原则”/“规则”，不同表述在本文中涵义上并无差别。

〔10〕 事实上，国内学界对“三重授权原则”指的是哪“三重”存在不同的解读。其中，数据获取方需取得用户的同意这点没有分歧，但另两重授权则有不同理解。王利明先生认为另两重指“第一次如果数据的收集者在收集信息的时候必须获得授权，第二次把收集到的信息进行分享的时候还要获得另一次授权。”参见王利明：《数据共享与个人信息保护》，载《现代法学》2019年第1期，第53页。薛军先生认为另两重指数据获取方需获得提供方的授权，以及提供方许可获取方获得数据需经用户的授权。参见薛军：《大数据时代数据信息权益的法律保护》，载《中国知识产权报》2017年4月19日，第008版。李安认为另两重指平台收集用户数据需经用户授权，第三方获取数据需经平台授权。参见李安：《人工智能时代数据竞争行为的法律边界》，载《科技与法律》2019年第1期，第64页。本文认为薛军先生的理解与判决书原文较为一致，故采此理解。

〔11〕 严格而言，此类案件属于数据使用纠纷，而非数据获取纠纷。但因数据使用与获取密切相关，比如企业间的数据使用规则(主要是限制性条款)往往在获取数据的合作协议中做出约定，一旦数据获取方违反约定将面临终止合作等后果，故数据使用“不当”会反过来影响数据获取。此外，若数据获取方将获得的数据再次授权给第三方使用(数据使用行为)，从第三方角度而言，则是数据获取行为。故本文将部分数据使用行为也纳入讨论范围。

〔12〕 该案目前尚未判决，初步查明的案件事实及法院观点可通过法院做出的行为保全裁定书了解。参见天津市滨海新区人民法院(2019)津0116民初2091号民事裁定书。

的已授权微信/QQ账号的登录服务提供给多闪产品使用，并不得以类似方式将其提供给抖音以外的应用产品使用；(3) 在多闪产品中使用来源于微信/QQ开放平台的微信/QQ用户头像、昵称等用户信息；(4) 在多闪产品中设置邀请QQ好友、邀请微信好友、一键邀请群好友功能按钮，诱导用户邀请微信/QQ好友使用多闪、注册抖音以及迁移微信/QQ群关系及好友关系。法院支持了前三项保全申请，但以不满足保全的紧迫性和必要性为由而否定了第四项行为的保全。法院认为，数据的使用是否合理、适当，应主要考量以下因素：一是数据持有企业和获取企业间的《开放平台开发者服务协议》；二是用户的知情权、选择权和隐私权等；三是个人信息的合理保护。法院在说理中再次重申了新浪微博案所提出的“三重授权原则”。

（二）企业数据获取中的主要法律问题

综合上述企业数据获取的典型纠纷可看出此类纠纷有如下特点：

第一，我国的企业数据纠纷中，原告都以“不正当竞争”主张自身的权益。这或许是因为我国目前立法中尚未明确承认企业对数据享有排他性“权利”，故企业无法直接以权利受侵害为由主张权利。

第二，企业数据纠纷不仅涉及争议双方企业，也往往涉及用户和社会公共利益，故法院裁判中往往将这些利益都纳入考量。然而，从法院说理来看，目前考量的重点往往在于用户利益和数据提供方利益，以及强调避免数据获取方“不劳而获”地取得市场竞争优势，对数据获取方利益、数据共享的社会价值及潜在的数据提供方限制作为竞争者的数据获取方的“不当”行为，则鲜有提及。

第三，“三重授权原则”成为判断企业间数据获取是否正当的重要标准。自“三重授权原则”在新浪微博案中被提出以来，该原则似乎已成为数据提供方主张数据获取方行为不当的“利器”，且该原则也对后续相关案件的裁判产生了重要影响。比如在上述腾讯与今日头条纠纷的裁定书中，法院认为“该原则已成为开放平台领域网络经营者应当遵守的商业道德”。〔13〕

第四，企业间的“开发者协议”成为法院认定数据获取企业行为是否妥当的重要依据。尽管此类“开发者协议”在实践中是由数据提供方单方提供，且相关条款对数据获取方往往较为不利，比如约定“一旦双方合作终止，数据获取方应立即删除所获得的所有数据”，但法院普遍承认了此类协议的效力，并要求数据获取方应完全遵守该协议。

基于上述特征可知，企业数据纠纷的主要法律问题是，如何对涉及相关当事人的利益和社会公共利益做衡量，而在具体判断上，则主要涉及不正当竞争行为的判断。其中，“三重授权原则”作为企业数据获取中的“特色”规则，值得认真对待，也是本文检视的重要对象。

“三重授权原则”系新浪微博案中二审法院提出的，针对第三方应用通过开放平台（如Open API）获取用户信息时应遵循的原则。该原则要求数据获取方在获取数据时既要获得用户的同意，同时也要获得数据提供方企业的同意。之所以需要二者的同意，是因为“数据在流动、易手的同时，可能导致个人信息主体及收集、使用个人信息的组织和机构丧失对个人信息的控制能力，造成个人信息扩散范围和用途的不可控”。而之所以要避免“不可控”是因为：其一，根据《消费者权益保护法》第29条等规定，“对用户个人信息的采集和利用必须以取得用户的同意为前提，这是互联网企业在利用用户信息时应当遵守的一般商业道德”。其二，“数据的获取和使用，不仅能成为企业竞争优势的来源，更能为企业创造更多的经济效益，是经营者重要的竞争优

〔13〕 事实上，新浪微博案被评为“2016年度北京市法院知识产权司法保护十大典型案例”，这表明司法系统对该案裁判规则的认可。

势与商业资源”。〔14〕

自“三重授权原则”提出以来,其不仅得到法院相关判决的遵循,也得到了学界不少学者的认同。比如王利明先生认为“此种做法值得赞同”。〔15〕薛军先生也认为“这一表述具有非常丰富的内涵,……法院在新浪微博诉脉脉案中阐发的针对个人信息保护,以及针对平台企业的数据信息权利的保护思路,比较好地平衡了各方主体的利益,对于我国未来个人信息保护以及数据信息产业的健康发展具有指导意义。”〔16〕

当然,也有学者并不认同这一原则。比如,许娟先生根据“风险决策树模型”认为,“三重授权原则不符合效益决策模型。……新浪诉脉脉案一、二审法院决策既不利于技术创新,也存在伪隐私保护的嫌疑”。〔17〕薛其宇先生从企业间数据竞争的规制角度认为,三重授权原则系从个人信息保护角度的规制方式,“个人信息保护规制的方法缺乏可行性及可操作性,难以有力规制数据不正当竞争行为。并且混淆了单独的个人信息与作为商业资源的个人信息的区别。因此,新浪诉脉脉案中的三重授权模式在数据不正当竞争的规制中并不合适”。〔18〕本文赞同三重授权原则“不利于技术创新和伪隐私保护”的批评,但将从不同角度对此做出论证。同时,本文并不认为“三重授权模式在数据不正当竞争的规制中完全不合适”,而是指出该模式在部分情境中是妥当的,但在多数情境中并不合适。

本文认为,三重授权原则是企业间数据流通的“高标”,即这是对企业获取数据提出的较为严格的要求,因为这一原则要求数据获取方需同时取得相关利害关系人——用户和数据持有方的同意。这一“高标”的优势在于为用户和数据持有企业提供了较强的保护。在目前个人对其信息、企业对其数据的权属尚不明朗的状况下,无论个人或企业对相关信息都无法享有“绝对权”属性的权利,三重授权原则通过当事人间的合意方式,有效消弭了潜在的诸多法律风险。但该原则的这一优势同时也是其弊端,即严格的数据获取要求可能限制数据的流通和开发,抑制企业创新和数字经济的发展,并导致企业运营成本和社会成本的增加等。〔19〕

基于上述对三重授权原则是“高标”的定位,一般而言,采该原则将有助于强化(至少不至于弱化)数据安全。但本文将论证,该原则仅应适用于有限的数据获取情形中。

二、获取可识别的原生数据无需企业同意之证成

本部分将论证,在数据获取方获得用户明确同意的情况下,该企业获取数据提供方相关用户的原生数据时,无须经数据提供方的同意。这是实务中争议最多的纠纷情境,也是本文最主要的主张。因本主张的数据范围仅限于可识别的原生数据,故下文将首先说明数据的分类,再证明本立场。

(一)数据的分类

关于数据的分类,目前最主要的分类方式是个人信息和非个人信息,是否“能够单独或者与其

---

〔14〕 北京知识产权法院(2016)京73民终588号民事判决书。

〔15〕 见前注〔10〕,王利明文,第53页。

〔16〕 见前注〔10〕,薛军文。

〔17〕 许娟:《互联网疑难案件中数据权利保护的风险决策树模型》,载《南京社会科学》2019年第3期,第83页。

〔18〕 薛其宇:《互联网企业间数据不正当竞争的规制路径》,载《汕头大学学报(人文社会科学版)》2018年第12期,第66页。

〔19〕 参见彭诚信:《独角兽法学精品·人工智能丛书之第二辑主编序》,载“规制与公法”公众号(https://mp.weixin.qq.com/s/ufRfeLCdW7mGpUgfX0nw8w,最后访问时间2019-08-19)。

他信息结合识别自然人个人身份”〔20〕是区分二者的标准。〔21〕此二者的区分价值在于，用户对个人信息享有诸多权益，但对非个人信息则无法主张。在个人信息中，又进一步区分为敏感信息和一般信息。国家标准《信息安全技术　个人信息安全规范》第3.2条规定，个人敏感信息指“一旦泄漏、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息”。二者区分的功能在于：对前者法律上更强调对用户的保护和“自决”，对后者则侧重于数据的开发利用。〔22〕对本文而言，上述分类的价值在于，在企业间数据流通时，用户对其个人信息享有一定的控制力。

但上述分类的不足在于：这些分类都是从个人角度出发，以数据与个人的关联程度而作的分类。鉴于本文关注企业间的数据纠纷，且实务中的纠纷往往发生于企业之间，而非用户与企业间，故企业对不同类型的数据享有何种不同权益对本文而言更具价值。基于此，本文采从企业角度出发对数据作分类。此种分类，目前学界大致有两种。

其一，是将数据分为基础数据和增值数据。基础数据是最本源的数据，即所有足以对主体构成识别的数据，用户作为个人数据的提供者，拥有个人基础数据的所有权。增值数据是指数据处理者对网络用户从事各种活动进行搜集整理等增值处理行为产生的各种数据，数据处理者享有经个人数据主体同意，并基于基础数据进行加工编辑分析而产生的增值数据所有权。〔23〕可见，这是以识别性作为区分标准。可以直接或者间接识别特定个人身份的数据是基础数据，基于用户同意而加工编辑分析而成的数据是增值数据。这种分类试图从企业角度做区分，但其脉络似乎仍然是参照了个人信息与非个人信息的区分。而所谓基础数据与增值数据的区分，事实上无法以识别性作为区分标准，因为增值数据也完全可能识别用户身份，比如对用户健康状况的评估结论数据，故识别性作为区分标准不足采。从上述基础数据和增值数据的描述来看，作者似乎是以数据是否经过企业的加工编辑分析作为二者的划分标准。

其二，是将数据分为原生数据和衍生数据。前者指不依赖于现有数据而产生的数据；后者指原生数据被记录、存储后，经过算法加工、计算、聚合而成的系统的、可读取、有使用价值的数据。〔24〕可见，这一分类是以数据的产生是否依赖于现有数据作为区分标准。依赖于现有数据，经过算法加工、计算、聚合而成的是衍生数据，企业对此享有权利；反之，不享有权利。

与前述的其他数据分类不同，原生数据和衍生数据的区分，有效地体现了企业对数据所投入“创造性劳动”的不同，而这是影响数据持有方在第三方获取其数据时，能否主张对数据控制力的重要因素。

综上，可识别性（个人信息与非个人信息）是影响用户对数据是否享有控制力的主要因素。是

---

〔20〕 参见《网络安全法》第76条第（5）项。

〔21〕 对于数据“可识别”存在分歧。主要担忧有二：一是数据反向识别技术等的发展导致数据是否可识别在“事实”上并非泾渭分明。二是“可识别”与否的“法律”认定标准不明。比如朱烨与百度隐私权纠纷案中，两审法院在cookie信息是否“可识别”问题上做出了不同判断，参见南京市中级人民法院（2014）宁民终字第5028号民事判决书。尽管就数据是否“可识别”仍存在诸多模糊空间，但鉴于我国在内的不少国家立法都已接受了“可识别”这一标准，本文将接受这一标准作为论证前提。

〔22〕 比如张新宝先生提出的“两头强化，三方平衡”理论，便是指“强化个人敏感隐私信息的保护和强化个人一般信息的利用”。参见张新宝：《从隐私到个人信息：利益再衡量的理论与制度安排》，载《中国法学》2015年第3期，第50页以下。

〔23〕 参见丁道勤：《基础数据与增值数据的二元划分》，载《财经法学》2017年第2期，第5页。

〔24〕 参见杨立新、陈小江：《衍生数据是数据专有权的客体》，载《中国社会科学报》2016年7月13日，第005版。

否依赖于现有数据(原生数据和衍生数据)是影响数据持有企业对数据是否享有控制力的重要因素。据此,本文将数据分为四类:可识别的原生数据、可识别的衍生数据、不可识别的原生数据以及不可识别的衍生数据。下文分别说明企业获取这四类数据的基本规则。

(二)可识别的原生数据无需企业授权的理由

可识别的原生数据指企业从用户处收集的,可识别用户身份的信息,比如用户的ID名称、头像、教育信息、网页浏览记录等。由于此类信息属于个人信息范围,故数据获取方从数据持有方处获取此类数据时需经用户同意,这是我国理论与实践的共识,也可从已有立法中解释出这一规则。比如,王利明先生认为:"数据共享之所以要取得数据权利人的同意,是因为数据共享本质上也是个人信息传输和收集的一种方式"。〔25〕我国已有的新浪微博案等,也提出了企业获取数据需经用户同意的要求。我国已有立法中虽没有条文直接提出这一规则,但立法中普遍存在企业收集用户数据需经用户同意的规定。〔26〕虽然这些规定所针对的典型情境是企业从用户处直接收集数据,但若将数据获取方获取数据的行为也解释为"收集、使用个人信息",则数据获取方也应遵循获得用户同意的规则。因此,可识别的原生数据共享需经用户同意,且这一同意为数据获取方从用户处获得的明确同意,当无疑问。

有疑问的是,此类数据的共享是否要经企业同意?目前我国的司法裁判和学界主流采肯定说,其理由主要有二。

其一,避免数据获取方"搭便车",削弱数据持有方的竞争优势。"相关的平台服务者通过自身的努力所获得的数据信息,也受到法律的保护,不允许他人搭便车,不劳而获。"〔27〕若数据获取方可不经持有方同意而获取数据,将导致"无正当理由截取了被上诉人微梦公司的竞争优势,一定程度上侵害了被上诉人微梦公司的商业资源"。〔28〕

其二,通过数据持有方这一"守门人"来提升用户的数据安全。比如,公安部发布的《互联网个人信息安全保护指南》第6.6条规定,共享和转让个人信息时需满足的要求之一是"在对个人信息进行共享和转让时应进行个人信息安全影响评估,应对受让方的数据安全能力进行评估确保受让方具备足够的数据安全能力,并按照评估结果采取有效的保护个人信息主体的措施"。可见,数据持有方要对获取方的数据安全能力"把关",以保障用户的信息安全。王利明先生甚至建议,"民法典有必要对信息共享中信息收集人和持有人保障个人信息安全的义务做出规定"。〔29〕

此外,学界主张企业数据权的学者提出的另一理由,是企业对其收集的数据享有排他性权利,故第三方获取数据需经其同意。关于企业数据权,本文将在第三部分展开详细分析,此处暂不展开。此处将论证,上述两项理由都难以成立,可识别的原生数据共享无需数据持有企业的同意,主要理由如下。

1."企业同意"规则的利弊衡量

诚然,若数据获取方无需数据持有方同意便可获得用户数据,将提升获取方的竞争力而相对

〔25〕 见前注〔10〕,王利明文,第47页。

〔26〕 比如,《网络安全法》第41条第1句规定:"网络运营者收集、使用个人信息,应当遵循合法、正当、必要的原则,公开收集、使用规则,明示收集、使用信息的目的、方式和范围,并经被收集者同意"。类似的规定,参见全国人大常委会《关于加强网络信息保护的决定》第2条第1段、《消费者权益保护法》第29条第1句等。

〔27〕 见前注〔10〕,薛军文。

〔28〕 北京知识产权法院(2016)京73民终588号民事判决书。

〔29〕 见前注〔10〕,王利明文,第56页。

削弱持有方的竞争优势。但这一论证存在如下不足。

第一，竞争力的此消彼长并不能直接得出法律应保护数据持有方竞争优势的结论。相反，通过法律保护自由市场中某一方企业的竞争优势并非常态，而是例外。正如法院在“大众点评诉百度地图案”中指出：“大众点评网上用户评论信息是汉涛公司付出大量资源所获取的，且具有很高的经济价值，这些信息是汉涛公司的劳动成果。”但是，“当某一劳动成果不属于法定权利时，对于未经许可使用或利用他人劳动成果的行为，不能当然地认定为构成反不正当竞争法意义上的‘搭便车’和‘不劳而获’，这是因为‘模仿自由’，以及使用或利用不受法定权利保护的信息是基本的公共政策，也是一切技术和商业模式创新的基础，否则将在事实上设定了一个‘劳动成果权’”。〔30〕基于此，竞争力的消长尚不足以成为支持数据持有方在数据流通中享有决定权的充分理由。

第二，数据获取方从持有方处获取数据并非“不劳而获”。应注意的是，若采数据获取方获取数据无需持有方同意的规则，并不意味着数据获取方可以自由地获取持有方的全部用户数据，因为获取方获取数据还需从用户处获得明确同意。比如，通过 Open API 获得新浪微博某用户的数据，需该用户明确授权脉脉获得其在微博的用户信息（需输入微博用户名和密码确认）。因此，只有数据获取方为用户提供了有着足够吸引力的产品或服务时，才能获得用户的授权，故数据获取方为用户提供的“优质”服务，正是其为获取用户数据所付出的代价之一。当然，从数据持有方的角度而言，数据获取方并没有为其提供“服务”，故数据获取方并没有对其支付“对价”。但这一推论成立的前提在于数据持有方对其数据享有“排他性”的权利或法律应予保护的正当利益。然而，正如上一段所指出的，这一“劳动成果权”目前并没有得到立法的认可，而主张“正当利益”的保护则负专门的论证义务。

当然，正如数据获取方需通过“优质”服务来获得用户的授权一样，数据持有方为收集数据也付出了可观的成本，故数据持有方对其收集的数据享有一定的权益应无可指摘，比如享有在法律和约定的范围内利用数据的权利。此处的问题在于，此种权益是否应包含对第三方能否获取其数据的决定权。这一问题的回答，需要比较不同制度安排对双方企业利益的影响，以及整体而言对社会的利弊得失。在价值层面，则主要体现为鼓励创新价值、市场自由竞争价值（既要制止不正当竞争，也要避免垄断）以及数据流通价值等之间的冲突与权衡。正如戴昕先生所指出的，“企业竞争维度上的机制设计相对更复杂，需要同时照顾到先发企业投资于收集、处理个人信息并基于此生产高价值数据资源的激励，以及后发企业充分利用现有资源寻求创新、避免形成垄断等市场竞争价值”。〔31〕

若采获取数据需经持有方同意的规则，无疑有助于保障数据持有方的竞争优势及相应的投资回报，进而鼓励创新和促进相关产业的发展。但这一规则的“副作用”同样不容忽视：数据持有方（往往是行业中处于优势地位的企业）可据此限制竞争者，乃至在一定程度上具有了影响哪些企业可进入相关市场的主导权，而这无疑会抑制创新且阻碍相关产业的发展。在正面与负面作用两相权衡下，本文认为该规则的负面作用更大，主要理由如下。

第一，允许无须数据持有方同意便可获取数据并不会严重抑制相关产业的投资与创新，因为：其一，由于网络外部性、锁定效应等原因，互联网领域有着“极强的‘强者恒强，赢者通吃’的

〔30〕 上海知识产权法院（2016）沪 73 民终 242 号。

〔31〕 戴昕：《数据隐私问题的维度扩展与议题转换：法律经济学视角》，载《交大法学》2019 年第 1 期，第 47 页。

竞争范式”，[32]故“抢占先机”对互联网企业而言尤为重要。比如网约车发展初期的滴滴与快的间的补贴大战，团购刚出现时的“百团大战”等，都是企业为占据某一新兴领域而“跑马圈地”的例证。基于互联网领域的这一特征，一旦用户规模已养成，其他企业想要再进入将异常困难，即便财大气粗如阿里、腾讯者，也往往采取的是收购而非推出类似服务的方式来进入该领域。故在实践中，企业不会因为后发企业可能获取其用户数据而不愿成为先发企业。其二，后发企业无法完全“掏空”先发企业的用户数据。即便后发企业获取数据无须先发企业同意，但其仍需经用户的同意。由于该同意需要具体用户的一一授权，很难想象后发企业能够在短时间内获得先发企业所积累的所有或大多数用户的授权，故先发企业的前期投入和竞争优势并不会因为数据可以被获取而付之东流。基于上述考量，采“获取可识别的原生数据无须企业同意”规则在实践中并不会严重抑制相关投资和产业发展。

第二，若要求“获取可识别的原生数据需经企业同意”，会不可避免地抑制数据获取方创新和产业发展，理由主要有以下四点。

其一，先发企业（数据持有方）会“本能”地拒绝向潜在的竞争者共享数据。尽管企业往往愿意标榜自身的共享美德，但数据的共享往往只发生在数据获取方与其无（潜在）竞争关系，不会威胁到其业务发展的前提下。比如在新浪微博案中，新浪微博长期以来允许脉脉通过Open API获取其数据，即便在新浪发现脉脉超过约定获取了用户职业和教育信息后，新浪也并没有立即终止双方间的合作。双方间的破裂，依被告脉脉的主张，肇始于新浪推出了其职场社交服务“微人脉”，与同样定位为职场社交软件的脉脉发生了直接竞争，而最终的触发，则因脉脉获B轮2000万美元融资。[33] 尽管先发企业为自身利益而试图限制后发企业无可厚非，但对行业整体而言，会限制占多数的后发企业的创新和发展。正如姚佳先生所言：“数据作为目前发展的关键性因素之一，其如能在本产业不同主体之间流动，必然有助于提升整个产业发展水准与良性生态。因此，建立一种企业数据利用分享规则与生态，也是当下的重要价值选择。”[34]此外，先发企业的此种拒绝，不仅会发生于有着直接竞争关系的企业中，也可能蔓延至没有直接竞争关系的企业，典型例证是腾讯微信与华为Magic手机之争。

其二，后发企业将更难进入相关市场领域。采“无须企业同意便可获取可识别的原生数据”的规则貌似“中立”，即任何企业都可能成为数据的获取方和被获取方，但在实践中的实施效果其实并不“中立”，相反，这是有利于初创期的中小企业成长与发展的规则。其理由在于：已经拥有众多用户的大企业往往无须收集其他企业的用户账户信息，而处于初创期的中小企业才会有此迫切的需求。比如新浪微博案中，被告在脉脉APP最初上线时，新浪微博账户是其唯一接受的用户登录方式，其甚至不提供手机注册等方式登录。因此，本规则表面上“中立”地促进企业间相互共享数据，但在实践中将演化为中小企业更便利地获取大企业用户信息的结果。这将有助于破除互联网领域的“强者恒强，赢者通吃”的垄断格局。反之，若获取数据以企业同意为前提，将可能导致先发企业只将数据共享给关联企业，进一步强化垄断格局。

---

〔32〕 网络外部性指互联网上产品的价值并不完全取决于产品本身的质量，而与使用该产品的用户数量紧密相关。使用该产品的用户规模越大，产品的价值就越大。锁定效应指用户在使用特定互联网产品以后，因网络外部性的作用而会被锁定在该产品网络中，用户若更换产品就需要放弃巨大的既得利益，或者付出较高的学习成本。参见孔祥俊：《反不正当竞争法新原理·分论》，法律出版社2019年版，第517～519页。微信是典型例证。“打败微信的，永远不可能是下一个微信”，即提供同质产品的后发企业无法替代先发企业。

〔33〕 参见北京知识产权法院（2016）京73民终588号民事判决书。

〔34〕 姚佳：《企业数据的利用准则》，载《清华法学》2019年第3期，第121页。

其三，当数据持有企业在某领域处于支配地位时，采“获取数据需经企业同意”的规则将导致数据持有企业事实上有权决定以此类数据为基础的各项创新能否展开，以及哪些企业可进入相关的行业领域。比如在腾讯与华为纠纷中，鉴于微信在即时通讯服务领域的垄断地位，若获取用户微信数据除了用户本人同意外，还需腾讯同意，则意味着以即时通讯服务数据为基础的各种创新能否展开将取决于腾讯的意愿。这在宏观层面可能抑制相关领域的创新和发展，在微观层面可能导致市场垄断。

其四，即便数据获取方获得了企业同意，其使用该数据往往受到持有方提出的诸多限制，且面临数据随时可能被“收回”的风险，影响数据的深度开发和企业的有序经营。目前实践中数据共享的做法是企业双方订立“开发者协议”等。由于此类协议多由数据持有方提供或主导，故无论是获得的数据范围、开发利用等，还是数据获取方，往往受到较多限制。比如，协议中的典型条款之一是，一旦双方合作终止，数据获取方要立即删除获得的所有数据。这在实务中将对数据获取方造成很大的困扰。比如，在新浪微博案中，在双方合作终止后，脉脉事实上花费了 6 个月时间才完成了将用户的新浪微博数据彻底清理的工作。〔35〕 在腾讯与头条案中，头条主张“采取保全将会影响被申请人的正常运营，给二被申请人造成不良社会影响和损害其声誉”。而原告腾讯也认可了“为保障该部分用户的利益免受影响，申请人明确表示将裁定生效前已通过微信/QQ 账号登录方式登录过多闪产品的用户排除在请求的保全措施之外”。〔36〕

综上，通过对“获取数据需要（不需）数据持有企业同意”规则的利弊衡量，“需经企业同意”规则对技术创新和产业发展造成的“副作用”在广度和深度上要高于该规则带来的正面“激励”效应。故“无须企业同意”应是更可取的选择。

需明确的是，若采取了“无需同意”规则，则在数据获取企业得到用户同意后，数据持有企业是否负有积极配合提供用户信息的义务，比如提供 API 接口的义务？本文并不主张数据持有企业负有此积极作为的义务，而是主张其只负有消极不干扰数据获取企业获取相关信息的义务，比如不采取技术手段阻止数据获取方获得相关用户数据等。但如果数据持有方已经向公众提供 API 服务，则基于非歧视原则，该企业不得在为其他企业提供 API 服务的同时，选择性地限制部分企业通过 API 获得相关用户数据。

采“无需同意”规则可能面临的一个现实问题是，这一规则是否会导致实践中掌握信息的数据持有方不愿再提供便利的数据共享服务，比如 API 服务，进而使得该规则的现实可行性打折扣。本文认为，这一规则并不会严重影响 API 等数据共享服务。其理由主要在于：其一，企业提供 API 接口，一般而言在商业上是“双赢”的结果。比如，提供 API 的企业可据此扩大自身的影响力，而使用 API 的企业则获得了相关用户信息等便利。正如法院在新浪微博案中所言，新浪微博“实施开放平台战略向第三方应用有条件地提供用户信息，目的是保护用户信息的同时维护新浪微博自身的核心竞争优势”。〔37〕 其二，利用 API 接口获取数据的企业，多数遵守“开发者协议”行事，故提供 API 的企业自然需考量是否为了避免少数的“逾矩”企业而取消整个 API 服务，毕竟这种选择有因噎废食之嫌。其三，即便有企业“逾矩”试图“过度”收集用户信息，数据持有方也可以获取方违背

〔35〕 双方合作自 2014 年 8 月 15 日终止，数据至 2015 年 1 月彻底清理完毕。参见北京知识产权法院(2016)京 73 民终 588 号民事判决书。

〔36〕 天津市滨海新区人民法院(2019)津 0116 民初 2091 号民事裁定书。

〔37〕 北京知识产权法院(2016)京 73 民终 588 号民事判决书。

法律规定的“必要性原则”〔38〕而限制该企业的信息获取行为。虽然某信息是否“必要”并非由提供API的企业单方界定,但在现实中其仍然掌握了一定的主动权,比如通过技术手段来限制数据获取方收集其认为超过“必要性原则”的数据。而数据获取方若欲主张其试图收集的信息符合必要性原则,则需通过主动磋商乃至诉讼来实现。基于上述考虑,可合理推测,“无需同意规则”并不会显著影响API等数据共享技术在实践中的运用。

另一可能的担忧是,若接受了获取数据无须企业同意的规则,是否会弱化用户数据的安全性。即未来企业在提供产品或服务时,会普遍要求用户同意其获得该用户在其他网站/软件中的数据,进而导致用户为获得企业的服务而大量暴露自己的信息给企业。这一担忧在实践中发生的可能性很低,原因至少有二。其一,企业获取数据需经用户的明确同意,这一同意在实践中一般表现为用户输入其相关的账号密码。比如企业若欲获得用户的微信数据,需用户主动输入其微信账号密码来验证并获得授权。因此,用户输入自己的各种账号密码来授权企业获取其在其他网站的信息在实务中一般不会发生,否则将是糟糕的用户体验。其二,需澄清的是,采获取数据无须企业同意,并不意味着数据获取方可以获得用户在数据持有方中的任何用户数据。鉴于我国在个人信息收集中采纳了“必要性原则”,即企业收集的用户信息应以必要为限,故数据获取方在获取另一企业的用户信息时,仍应以必要为限。若数据持有企业认为获取方要求获取的用户信息超过了必要的限度,可以拒绝获取方获取相关信息。当然,基于获取方希望尽可能广泛地获取用户信息和持有方希望限制用户信息共享的现实动机,这样的规则会导致何为“必要信息”成为实践中双方争议的焦点之一。在双方的不断“拉锯”中,可以合理期待“必要信息”在各具体场景中的“习惯”会逐渐形成。因此,“无须企业同意”规则并不会导致用户数据的大量暴露。

2.“企业同意”规则无助于强化用户保护

在企业获取数据的规则设计中,始终要考量的因素之一是对用户个人信息/隐私权的保护。正如姚佳先生所言:“无论如何进行价值与利益衡量,充分保护个人信息都是‘底线’与终极价值,不容撼动。”〔39〕因此,保护用户个人信息也成了“企业同意”规则的理由之一,即由数据持有方作为用户利益的“守门人”。在企业数据纠纷中,保护用户隐私这面“大旗”始终被数据持有企业反复提起和强调,尤其是在我国立法尚未确认企业数据权利的当下。同时,用户隐私保护也是法院裁判时选择支持数据持有方主张的重要考量因素。但本文此处将揭示,企业在保护用户个人信息方面存在明显的“言行不一”现象,“企业同意”规则并不能有效提升对用户的个人信息保护,企图由数据持有方来为用户利益把关并不可行。

尽管数据持有企业在纠纷中总是强调其对用户隐私的重视与保护,但若对照企业的实际行为,常会发现“言行不一”现象。以新浪微博诉脉脉案为例。尽管原告新浪微博主张其为了保护用户隐私而终止了与脉脉的合作,但原告的多项行为表明,其对用户隐私其实并非如此“关心”。〔40〕其一,脉脉获得的是API普通接口,本无法获得微博用户的教育信息和职业信息,但新浪微博却因自身的技术漏洞而让脉脉可以直接获得此类信息,表明新浪在保护用户数据的技术上并未给予足够重视。其二,新浪在发现脉脉超过双方间协议约定的范围收集微博用户的信息后,并未立即在

〔38〕 比如《网络安全法》第41条前段规定:“网络运营者收集、使用个人信息,应当遵循合法、正当、必要的原则。”《消费者权益保护法》第29条也有类似的规定。

〔39〕 见前注〔34〕,姚佳文,第118~119页。

〔40〕 下述事实均来自新浪微博诉脉脉案的判决书,参见北京知识产权法院(2016)京73民终588号民事判决书。

技术上予以弥补或要求脉脉纠正，而是要求脉脉共享其用户信息给新浪作为交换。在该要求被拒绝后，才禁止了脉脉的 API 接口。正如一审法院所评价的，新浪这是“在发现第三方应用软件发生非法抓取使用微博用户信息的情况下，以他人利益作为交换条件，放纵不正当竞争行为”。其三，新浪主张脉脉非法获取并使用脉脉注册用户的手机通讯录联系人与新浪微博用户的对应关系，且在脉脉软件中予以展示。但事实上，新浪自己提供的微博服务和微人脉软件，也同样存在获取用户手机通讯录信息并匹配相应的微博用户，且在软件中予以展示的行为。最后，新浪主张脉脉的违法行为之一，是脉脉通过“脉脉”“淘友网”两个微博账号大量读取微博用户的职业和教育信息，非法抓取、使用了新浪微博用户信息，侵害了微博用户的信息权益。然而，新浪与其用户订立的《微博服务使用协议》中第 6.2 条却约定：“微梦公司保证不会将单个用户的注册资料及用户在使用微博服务时存储在微梦公司的非公开内容用于任何非法的用途，且保证将单个用户的注册资料进行商业上的利用时应事先获得用户的同意，但下列情况除外：……6.2.4 用户自行在网络上公开的信息或其他已合法公开的个人信息”。这一约定表明，新浪认为其可无须用户同意而使用用户自行在网络上公开的信息。但却主张脉脉的相关行为侵害了用户的信息权益。综上可见，新浪微博对脉脉行为的指摘，与其自身的诸多行为并不一致。故保护用户隐私是否真的是新浪起诉脉脉的动机之一，颇值怀疑。

其实，本案中不仅新浪言行不一，被告脉脉又何尝不是。比如，脉脉公司创始人林凡在微博上称，“我的人生面临过很多次纠结，但这一次选择，只用了 1 秒钟。理由很朴素：用户在脉脉的隐私资料，不可能在未经用户授权的情况下，以任何形式、任何理由，提供给任何第三方。脉脉决定：关闭微博登录……”虽然林凡自称是为守护用户隐私而拒绝了新浪微博的要求，但脉脉漠视其与新浪微博间的合作协议，通过 API 竭尽所能地获取微博用户信息的行为，与其宣称坚持的价值南辕北辙。

若观察企业数据之争，会发现绝大部分纠纷都存在着企业言行不一的现象。比如腾讯与华为的数据之争。腾讯认为华为获取并利用微信用户聊天数据等行为侵犯了微信用户的隐私，即便华为已获得了用户的同意。但在此事件中对用户隐私“颇为敏感”的腾讯，本身也从事着挖掘利用用户数据的行为，比如在微信朋友圈中发布的广告，便是分析了用户微信数据后做个性化投放。因此，若承认微信朋友圈的广告精准投放行为合法正当，则主张华为行为侵害了用户隐私便显得“只许官家放火，不许百姓点灯”。

同样，在腾讯诉今日头条案中，腾讯主张抖音在向用户推荐好友时使用了来源于微信/QQ 的用户头像和昵称，及抖音将其获得的用户微信数据共享给多闪等行为，侵害了用户隐私。但腾讯的微信和微视软件却也从事着类似的行为。在王先生诉腾讯案中，王先生主张，微信/QQ 将其用户信息共享给了腾讯旗下的微视软件，以帮助微视提供更精准的服务。具体而言，当用户使用微信/QQ 账号登录微视软件时，微视软件不仅会收集用户的注册信息等以验证用户身份，而且会获取用户在微信中的好友信息，并向用户推送好友发布的视频。香坊区法院做出了腾讯立即停止在微视中使用王先生的微信/QQ 好友信息，并立即停止将王先生的相关信息推荐给其他用户的行为保全裁定。〔41〕

为何会普遍存在上述“言行不一”的现象？一种可能的解释是，数据持有企业是以保护用户隐

〔41〕 参见王巍：《微视自动获取好友信息，用户申请停止使用获法院支持》，载《新京报》2019 年 7 月 2 日（http://www.bjnews.com.cn/news/2019/07/02/598162.html，最后访问时间 2019－08－19）。目前该案件还在审理中。

私之名，行限制对手竞争之实。比如，在新浪微博案中，原被告间的数据合作关系长期存在，而当原告开始推出职场社交软件“微人脉”，与被告提供的服务重叠后，原告便对被告获取数据提出更严格的要求。此外，原告曾一度希望被告提供其用户数据给原告旗下的“微人脉”，以作为被告获取原告微博用户数据的交换。可以想象，若被告接受了原告的这一提议，或许就不会有此诉讼，原告在诉讼中对被告行为的诸多指摘可能也就放过了。因此，原告的诉讼动机并非保护用户隐私，而是为了限制竞争对手，实现自身商业上的扩张。

企业以保护用户隐私之名行排斥竞争之实在美国的hiQ案中曾被法官明确指出。与我国案件不同，该案是数据获取方hiQ起诉了数据持有方LinkedIn，主张被告不得禁止其抓取被告网站上公开发布的用户数据。该案中的被告LinkedIn也声称自己禁止原告抓取其用户信息的目的，是出于保护用户隐私的考量。但LinkedIn的这一主张并不“可靠”，比如，在另一案件中，LinkedIn曾主张其用户对其公开发布的信息并不享有隐私利益。因此，LinkedIn的保护用户隐私主张并没有被法院接受。相反，法院认为更应支持原告hiQ的主张，即LinkedIn的行为目的在于排斥hiQ作为竞争者进入数据分析领域，可能违背了反垄断法(Sherman Act)的政策与精神。[42]

综上，企业对用户隐私/数据的保护，是以自身利益，而非用户利益，为核心考量。在限制对方获取和利用用户数据有利于其排斥(潜在)竞争者时，高举保护用户隐私的大旗；而在获取和利用用户数据有助于提升自身的产品/服务时，则尽可能广泛地获取用户数据，对所谓的用户隐私视而不见，或已获得了用户许可为由一笔带过。企业的这一做法，其实是在法律没有赋予企业数据权利的情况下，以保护用户隐私为名而实现对数据的排他性权利的一种策略。

基于上述分析，在信息流通中寄希望于由企业来把关和维护用户数据安全的想法并不可行，且这无法通过提升企业的自律程度、道德水准或法律的强制性要求而完全解决，因为这一规则违背了“任何人不得为自己法官”的基本原理。数据持有企业并不是超脱于用户和数据获取企业之外的第三方，相反，其利益深深地嵌入其中。故数据持有企业不可能基于维护用户利益，而非基于自身利益，做出相关决策行为。此外，“企业同意”规则不仅无助于强化对用户的保护，还会造成排斥市场竞争等弊端。

3. 比较法考察：欧盟和美国的经验

第三方企业获取数据持有企业的数据，需经数据持有企业的同意，这是我国当前实务界的通行做法，似乎“理所当然”。但若考察美国和欧盟的情况，可发现这并非是显而易见的结论。

在欧盟，数据共享(data sharing)领域尚没有直接明确的法律规则。根据一份提交给欧盟执委会(European Commission)的报告显示，法律对数据所有权(data ownership rights)不明确，企业对数据可采取的合法处理行为不明确，以及难以追踪和控制被共享的数据，是目前欧盟在数据共享问题上面临的主要法律障碍。[43] 虽然欧盟还没有明确的数据共享规则，但欧盟《数据保护条例通则》(General Data Protection Regulation)中规定的数据可携权(right to data portability)或许可以为企业间的数据流通提供启示。

数据可携权由欧盟《数据保护条例通则》第20条确立。第20(1)规定：“数据主体有权获得由他/她提供给数据控制者(controller)的，与其相关的个人数据，该数据应是结构化、被普遍采

---

〔42〕 See *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F.Supp.3d 1099, 1118 (N.D.Cal. 2017).

〔43〕 See Everis Benelux, “Study on Data Sharing between Companies in Europe (Final Report)” (https://publications.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en/format-PDF/source-101964902, last access 2019-07-10).

用且机器可读的格式。数据主体有权将这些数据无障碍地从原数据控制者传输给其他数据控制者。”数据可携权的规范目的是“强化数据主体并赋予主体在相关个人数据上更多的控制力”，同时该制度是“一种重要的支持个人数据在欧盟自由流通并促进数据控制者之间竞争的途径。该制度将方便数据主体在不同服务提供者之间转换，从而在欧盟数字单一市场战略下，促进新服务的发展”。〔44〕

虽然数据可携权的首要出发点是强化对用户的保护，其制度设计也是赋予用户权利，但这一制度对企业数据流通的规则设计同样有借鉴意义。因为这一制度的目标之一是限制企业对用户数据的排他性控制，从而促进数据流通、企业竞争及数字经济发展。有学者甚至认为，“数据可携权与数据保护法的基本权利属性并不完全契合，相反，其应被视为是欧盟为了促进数据驱动市场(data-driven markets)竞争和创新的一种新规范途径”。〔45〕

如果数据可携权所体现出的价值选择是可取且可行，〔46〕则本文所主张的“无须企业同意”规则亦应得到支持，因为二者的实践效果相似，即在用户同意的情况下，用户数据从一家企业转移到了另一家企业。二者的区别主要在于：数据可携权是从用户的角度赋予的权利，数据因用户的请求而发生移转；本文主张的规则是从企业角度的设计，在第三方企业获得用户许可后，有权获得用户在数据持有企业的数据而无须该企业许可。

此外，数据可携权所涵盖的数据范围对本文也有参考价值。从《数据保护条例通则》第 20 条第(1)项的规定可看到，用户可基于可携权而获得/传输的数据有两个要件：由主体提供且与主体相关。对此二要件的理解，欧盟数据保护工作组(Data Protection Working Party)作了较为宽泛的理解。根据工作组发布的指南(以下简称“指南”)：(1) “与主体相关”意味着任何匿名数据或与该数据主体无关的信息都不在可携权范围内。当数据涉及数据主体之外的第三方，比如通讯录联系人信息，仍应在可携权范围内。只不过获得数据的新数据控制者不得侵害第三方的权利，比如基于市场推广目的而向第三方发送广告信息。(2) “由主体提供”应作广义理解，包括：一是由主体主动、有意提供的数据，如用户名、年龄等；二是由用户使用服务或产品而产生的并可监测到的数据，如用户搜索历史、地理位置信息以及通过可穿戴设备得到的心率数据等。(3) 若与数据主体相关的数据同时涉及知识产权或商业秘密，数据控制者也不得据此拒绝数据主体的请求。但可携权的数据范围并不包括数据控制者基于“由主体提供的信息”而创造的推断数据(inferred data)和衍生数据(derived data)，比如对用户健康状况的评估结果数据。〔47〕

由此可见，数据可携权所涵盖的数据范围非常宽泛，其主要的判断标准，在于数据是否由数据主体“提供”。从指南的表述来看，“提供”似乎可理解为：用户参与了数据的产生，无论该参与是直接提供，抑或是被技术设备所收集。指南的这一界定，与本文主张的可识别的原生数据范围相似。本文的原生数据与衍生数据，是以数据的产生是否依赖于现有数据为区分标准，其核心在于区分企业对数据所投入的“创造性劳动”的不同。本文分类与可携权的差别在于：本文是从企业角度所

---

〔44〕 Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, 16/EN WP 242 rev.01, 3 (2017).

〔45〕 Inge Graef, Martin Husovec & Nadezhda Purtova, *Data Portability and Data Control: Lessons for an Emerging Concept in EU Law*, 19 German L.J. 1359 (2018).

〔46〕 对数据可携权当然不乏批评之声，主要的批评来自其规范目的能否实现及其可能高昂的实施成本。*See* Peter Swire & Yianni Lagos, “Why the Right to Data Portability likely Reduces Consumer Welfare: Antitrust and Privacy Critique”, 72 Md. L. Rev. 335 (2013). 但肯定意见似乎仍是主流。

〔47〕 See *supra* note〔44〕, at 9 - 12.

做的分类，而可携权是从用户角度所做的界定。但二者所涵盖的具体数据内容，则基本重叠。这为本文的主张提供了比较法上的支撑。

在美国也有着类似欧盟可携权的制度安排。“数据红利共享制度”也起到了允许用户在不同服务提供者间传输数据的效果。比如2011年美国首席技术官要求工业必须“以在线且可被机读(machine readable)的方式公布用户数据，并且不能限制用户对这些数据的再利用。”[48]这意味着，用户可以从初始企业获得其可被机读的数据，然后在其他企业提供的服务上使用该数据，该再使用行为无须经过初始企业的“授权”。可见，美国的数据可机读化制度与欧盟的可携权在实践中发挥了相似的作用，这进一步强化了本文的比较法基础。

当然，美国的企业数据之争，主要体现于其判决中。从已有的判决来看，数据持有企业若欲禁止第三方获取其数据，可能的诉因(cause)有：侵权中的干涉动产侵权(trespass to chattels)、《计算机欺诈与滥用法》(Computer Fraud and Abuse Act)中的未经/超越授权进入系统(without authorization or in excess of authorization)、违约、侵害版权以及反垄断和不正当竞争。尽管干涉动产是此类案件早期主要的诉因，但在1994年《计算机欺诈与滥用法》允许提起民事诉讼后，该法逐渐成为企业诉讼的主要诉因。法院在认定当事人是否未经/超越授权进入系统，以及是否构成垄断和不正当竞争上，存在分歧。部分判决在说理或裁判的实践效果上支持了本文的主张，部分则与本文相左。

Facebook诉Power Ventures案是与本文观点部分相左的案件之一。被告Power Ventures为用户提供聚合其社交软件账户的服务，即用户登录Power Ventures账户，并授权被告获取其在Facebook等各社交软件的信息。这样，用户可以只登录被告网站就能追踪各社交网站的信息。在被告向Facebook用户推广其服务被Facebook意识到后，Facebook向被告发送了禁止信(cease and desist letter)，要求其停止推广服务，并签署“开发者协议”。被告拒绝后，原告通过IP技术禁止被告获取其网站上的用户信息。被告则采取了改变IP地址的方式继续获取信息。之后，原告以被告违反《计算机欺诈与滥用法》等为由提起诉讼。地方法院支持了原告的所有诉讼请求，但上诉法院则作了一些调整。第九巡回法院认为，在原告发送“禁止信”前，被告有理由认为，在获得原告用户的同意后，其有权进入原告的计算机系统。但在原告发送“禁止信”后，被告仍然进入原告系统违反了《计算机欺诈与滥用法》。法院在说理中认为，“Power要想继续通过Facebook系统来推广其服务，需同时获得Facebook具体用户(作为数据和个人页面的控制者)和Facebook(数据存储于其服务器上)的同意。在Facebook发送禁止信后，仅仅拥有用户的同意并不足以允许其继续进入系统”。[49] 可见，Facebook案中法院认为同时获得用户和数据持有方同意是第三方企业获得数据的必要条件。

但美国也同样存在不同于上述判决的案件，hiQ案是典型。在hiQ案中，原告hiQ从被告LinkedIn网站抓取了LinkedIn的用户数据，并对获得的用户数据做统计分析后销售，比如通过分析用户在LinkedIn发布的信息来推断哪些用户存在离职倾向，并将该结论销售给其雇主。[50] 在hiQ案中，hiQ收集并使用用户的数据既未经用户同意，也未经数据持有企业LinkedIn同意，但最终法院判决LinkedIn不得禁止hiQ从其网站收集用户数据。在涉及《计算机欺诈与滥用法》时，法

---

〔48〕 See Aneesh Chopra, “Remarks to Grid Week”, 转引自龙卫球：《数据新型财产权构建及其体系研究》，载《政法论坛》2017年第4期，第72～73页。

〔49〕 *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1062－1068 (9th Cir. 2016).

〔50〕 See *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F.Supp.3d 1099 (N.D.Cal. 2017). 该案仍在上诉中。

院认为，hiQ 案与 Facebook 案等已有案件的主要差别在于：本案所涉的用户数据是公开的数据。根据《计算机欺诈与滥用法》的立法史和规范目的，其主要是为应对黑客行为，故该法中的“授权”应仅限于须认证的系统，比如需输入密码的系统。

美国的上述两个典型案件，与我国已发生的企业数据之争案件都不完全相同，但仍不乏参考价值。Facebook 案法院直接指出被告 Power Ventures 若欲获取原告的用户信息需经用户与 Facebook 的双重同意。但需注意的是，两项同意的基础并不同。需经用户同意，是因用户是数据和个人页面的控制者，即用户是数据的权利人。但之所以要获得 Facebook 同意，并不是因为 Facebook 对数据享有某种权利，而是因为数据存储于其服务器上。被告 Power 也不是因为侵害了 Facebook 的数据权而承担责任，而是因为未经授权进入了 Facebook 的系统，即这一主张的法律基础是侵权法上的“干涉动产侵权”。在我国，“干涉动产侵权”并不是一种独立的侵权类型，已有的司法实践也未见有判决将未经许可进入企业的计算机系统作为一种侵权行为对待。〔51〕 我国判决中法院支持数据持有方的理由，往往是企业“对基于自身经营活动收集并进行商业性使用的用户数据整体同样享有合法权益”。〔52〕 因此，从企业对数据享有的权益角度而言，Facebook 案其实并没有支持我国法院赋予数据持有方对数据享有一定的控制权的做法。当然，若从“功能等同”的角度而言，该判决确实与本文主张不同。至于 hiQ 案，美国法院提出的获取数据无须用户和企业同意的观点，尽管与本文主张不同，但“举重以明轻”，该判决关于无须企业同意的理由，也在一定程度上支持了本文的主张，只是本文并不同意该判决关于获取数据无须用户同意的论证。〔53〕

综上，比较法的经验确实在一定程度上支持了本文主张的“无须企业同意”规则。

三、获取其他类型数据的规则

除上文的“可识别的原生数据”外，其他类型数据的获取规则相对易于达成共识，本文只作简要论证。

第一，获取非可识别的衍生数据无须取得用户同意，但需取得企业同意。获取非可识别的衍生数据无须取得用户同意，这一点当无疑问，因为数据无法识别用户身份，自然无法获得用户同意。主要的问题在于，此时是否需数据持有企业同意。对此问题的回答，典型的思路是，先确定企业对衍生数据享有何种属性的权利，之后确定具体的权利内容，即“数据权属是数据利用和流通及数据产业化的逻辑起点”。〔54〕

关于企业数据权，国内的主张主要有两类：一类是赋予企业对其收集的用户数据广泛地享有权利；另一类是对企业持有的数据做分类，然后主张企业对部分类型的数据享有权利。吊诡的是，目前第一类观点主要由学界学者主张，而第二类观点主要由实务界人士主张。

在学界，关于企业的数据权利属性，有新型财产说、知识产权说、原始取得说等。龙卫球

〔51〕 但我国已将非法进入计算机系统或获取公民个人信息纳入刑事责任，参见《刑法》第 285 条和第 251 条之一。刑事（而非民事）先行是我国个人信息保护领域的一个特点。

〔52〕 参见天津市滨海新区人民法院（2019）津 0116 民初 2091 号民事裁定书。

〔53〕 从美国学界对该案件的评论来看，较少关注“用户同意”的探讨，而主要聚焦于“企业同意”问题，且不乏对该案判决的支持者。See Jamie L. Williams, “Automation is not ‘Hacking’: Why Courts must Reject Attempts to Use the CFAA as an Anti-competitive Sword”, 24 B.U. J. Sci. & Tech. L. 416 (2018).

〔54〕 见前注〔23〕，丁道勤文，第 5 页。

先生认为，针对数据应分别构建自然人的关于个人信息的权利和企业的关于数据的权利，后者统称为企业新型数据财产权，具体包括数据资产权和数据经营权两种形态。数据资产权的客体，是具有特定功能或者利用价值的数据集合或者数据产品。数据资产权作为一种专有排他权，比对所有权、知识产权来设计，其私益结构部分，体现为企业对其数据在特定范围享有占有、使用、收益和处分的权利。〔55〕许可先生也认为，数据权“意指数据控制者对‘数据集合’(collection of data)享有的占有、处理、处分的权利”。数据集合指“通过计算机技术形成的、以二进制信息单元0/1表示的半结构化或多结构化巨量电磁记录。与‘数据库’不同，它不需要经过严格逻辑汇编也即‘结构化’，亦不要求原创性，并在规模、种类、更新的及时性和速度等方面远超前者。”〔56〕依此论述，企业数据权所涵盖的数据范围相当广泛，凡是企业数据集合中的数据，都可纳入数据权而予以保护。同时，企业数据权的权利内容也包罗万象，企业可对与数据相关的各方面利益享有广泛的控制力。

与国内学界试图对企业所持有的数据广泛地赋予数据权不同，国内实务界人士对企业数据权的主张则要“谦抑”得多。正如本文“数据的分类”部分所介绍的，实务界试图对数据做区分，并对不同类型的数据主张不同的权利。比如丁道勤先生将数据分为基础数据和增值数据。对基础数据，用户作为数据的提供者，拥有个人基础数据的所有权；对增值数据，数据处理者享有基于基础数据进行加工编辑分析而产生的增值数据所有权。〔57〕同样，杨立新先生和陈小江先生将数据区分为原生数据和衍生数据，二者区分的主要价值在于：企业对后者享有绝对性权利，即应以衍生数据为客体建立数据专有权，该权利是一种财产权，性质上属于一种新型的知识产权。〔58〕其实，尽管丁道勤先生将数据是否可识别作为区分基础数据和增值数据的标准，但从其具体阐述来看，其似乎也主要以数据是否经企业加工编辑作为区分的实质标准。若作此理解，则该区分与原生/衍生数据的区分并无不同。

综上可见，尽管学界在企业是否对用户个人信息享有权利方面存在分歧，但在经企业加工产生的衍生数据方面，则有共识：企业对此类数据享有一定的排他性的权利。据此，获取非可识别的衍生数据需经企业同意，应是共识。

就为何企业可对其通过数据挖掘技术后得到的衍生数据享有排他性权利，学界的解释一般是基于促进产业发展的考量。就理论解释层面，企业挖掘数据的行为可解释为“加工”，故企业可基于加工这一事实行为取得对衍生数据的权利。更进一步，即便企业加工所依赖的“原料性”数据来源并不合法，其加工的事实行为也可能使企业对该衍生数据享有权利，即此时第三方企业若欲获得数据，仍需获得数据持有企业的同意。

第二，获取可识别的衍生数据需同时获得用户和企业的同意。理由在于：一方面，因为数据可识别，故需获得用户同意。另一方面，作为衍生数据，需获得企业同意。故获取此类数据需同时获得用户和企业同意。

第三，获取非可识别的原生数据无需用户同意，是否需企业同意应视数据是否公开而定。一方面，因为数据非可识别，故无需经用户同意。另一方面，若此类数据并未公开，则不应允许数据

〔55〕 参见龙卫球：《再论企业数据保护的财产权化路径》，载《东方法学》2018年第3期，第52、60页；另见前注〔48〕，龙卫球文，第75页。

〔56〕 许可：《数据保护等三重进路——评新浪微博诉脉脉不正当竞争案》，载《上海大学学报(社会科学版)》2017年第6期，第23页。

〔57〕 见前注〔23〕，丁道勤文，第5页。文章发表时，丁道勤的身份是京东集团法务部政策研究总监。

〔58〕 见前注〔24〕，杨立新、陈小江文。文章发表时，陈小江单位系阿里巴巴集团公司法务部。

获取企业自由获取或要求持有企业提供数据，因为此时数据获取企业缺少了“用户同意”这一获取数据的正当性基础。但若此类数据被公开，或数据持有企业并未采取技术措施来避免其被获取（事实上公开），则此时应允许其他企业自由获取数据。其理由主要有二：一是学界对原生数据是否应赋予数据权利尚无共识，在此情况下本文认为不宜赋予数据持有企业较强的数据控制力；二是基于促进数据流通和企业竞争的考量，对无关用户的“非可识别”数据，应以数据的充分流通和挖掘为优先考量。当然，这并不意味着数据持有企业在获取非可识别的原生数据上的投入将被其他企业自由地搭便车。只要数据持有企业对此类数据采取一定的措施避免其公开，其仍可享有此类数据带来的相关利益。

四、企业数据获取类型化规则的适用

根据本文的论证，企业数据获取应区分不同数据类型而采不同规则，具体如下。

表 1　数据类型及相应的数据获取规则

数据类型	可识别的原生数据	非可识别的原生数据	可识别的衍生数据	非可识别的衍生数据
数据类型例证	用户名、头像	匿名问卷的答复	用户健康状况评估	“双 11”各省消费者网购金额
数据获取规则	需用户同意；无须企业同意	无须用户同意；是否需企业同意视公开与否而定	需用户且企业同意	须企业同意；无须用户同意

对上述规则，补充说明三点：（1）目前被法院广泛接受的三重授权原则，其适用范围应做大幅限缩。只有在获取可识别的衍生数据时，才适用三重授权原则。（2）上述规则，只适用于与用户“有一定关联”的数据，并不包含实务中所有的数据类型。所谓“有一定关联”，指数据由用户提供（既可以是可识别身份，也可能是无法识别身份），或数据在用户提供的基础上“加工”而成。实务中除本文所涉的数据外，还包括与用户无关的数据，比如法律法规、司法判决、报刊等数据。对这些数据，以及由这些数据所组成的数据库，有着一套相对独立的规则，[59]并非本文探讨的数据规则所适用的对象。换言之，本文所提出的数据获取规则，并不能涵盖实务中所有的数据情形。（3）需注意区分数据和数据库。现实中可能出现原生和衍生数据相结合而成的混合数据库，即数据库中的部分数据直接源于用户提供，部分源于企业计算、加工等。但对某一数据而言，不存在混合的情形。本文是从数据（而非数据库）角度探讨数据获取问题。

根据上述规则，国内的典型企业数据纠纷，可作如下法律判断。

第一，大众点评诉百度地图案。百度在获得大众点评网上的用户评价信息时，并未获得用户同意，故该行为不应得到支持。法院认为百度构成不正当竞争应予支持。

第二，腾讯与华为事件。鉴于华为在获取用户的微信聊天记录前已获得了微信用户的同意，且用户的微信聊天记录属于原生数据，故华为获取该数据无须再获得腾讯的许可，腾讯不得以侵害其企业数据为由禁止华为的数据获取行为，更无法以保护用户隐私来正当化自己的主张。当然，现实中可能出现的一种情况是，手机用户主体与微信用户主体并不一致，即华为获得的用户许可与微信用户并非同一主体。此时华为无权获取微信用户信息。但鉴于两类主体同一的可能性

〔59〕 此类数据/数据库的规则多见于关于“数据库”的研究中。

在绝大多数情况下成立，故若腾讯作此主张，应负举证责任。

第三，新浪微博诉脉脉案。新浪微博主张的多项不正当竞争行为，评价如下：（1）被告脉脉在双方合作期间超出API许可范围抓取并使用了脉脉用户在微博上的职业、教育信息。由于脉脉已获得用户同意，〔60〕且职业、教育信息属于可识别的原生数据，故脉脉可获得该数据，无须以新浪同意为前提。同样，在双方合作结束后，脉脉也仍可使用这些微博用户数据。脉脉的这些行为不应被认定为不正当竞争行为。〔61〕当然，新浪微博若欲否定脉脉的行为，还可尝试另一主张是：脉脉对微博用户职业、教育信息的收集，超过了“必要限度”，违背了信息收集的必要性原则。〔62〕（2）脉脉未经新浪同意，绕过API获取非脉脉用户的新浪微博数据。由于未经用户同意，故该行为不应得到支持。

第四，腾讯微信/QQ诉头条抖音/多闪案。该案中，腾讯的主张至少有三：一是禁止抖音向用户推荐好友时使用来源于微信/QQ开放平台的微信用户头像、昵称；二是禁止抖音将通过微信/QQ开放平台获得的数据授权给多闪使用；三是禁止多闪使用微信的用户头像、昵称。腾讯的上述主张，涉及第三方企业获得数据持有企业的数据后，在数据使用方面的行为规则。这一问题虽与本文所论证的获取规则并不相同，但本文的获取规则对此案件的裁判仍不乏启示意义，理由在于：本文主张第三方企业在获得用户同意后，获取数据无须数据持有企业同意，举重以明轻，第三方企业对获得的数据的使用，数据持有企业更无权置喙。当然，这并不意味着第三方企业可对获得的数据为所欲为，该企业仍需遵守法律上关于个人信息保护的规则，并受用户协议的约束。此外，鉴于头条公司所使用的是微信用户头像、昵称信息，此类信息属于用户的基本信息，难谓逾越了数据收集的“必要性原则”。据此，腾讯公司的上述主张不应得到支持。〔63〕

除了司法裁判外，我国相关规范性文件也应作相应调整。

其一，应增设关于企业间数据流通（共享）的规则，而非将此类规则“寄居”于个人信息保护规则中。企业间的数据流通规则与个人信息保护规则并非仅仅是“一体两面”的关系，因为非可识别的信息属于企业数据但并非个人信息，且企业对可识别的衍生数据也享有一定的权益，另外不同角度下的数据/信息表达也不同，〔64〕故通过个人信息规则并不能完全涵盖和解决企业数据流通问

---

〔60〕 脉脉与其用户订立的《脉脉用户协议》第2条中约定：“第三方平台记录信息”定义为“用户通过新浪微博账号、QQ账号等第三方平台账号注册、登记、使用脉脉服务的，将被视为用户完全了解、同意并接受淘友公司已包括但不限于收集、统计、分析等方式使用其在新浪微博、QQ等第三方平台上填写、登记、公布、记录的全部信息。用户一旦使用第三方平台账号注册、登录、使用脉脉服务，淘友公司对该等第三方平台记录的信息的任何使用，均将被视为已经获得了用户本人的完全同意并接受。”参见北京知识产权法院（2016）京73民终588号民事判决书。

〔61〕 当然，新浪微博与脉脉间订立的《开发者协议》中有约定，脉脉可通过API获得的数据范围并不包括微博用户的职业、教育信息。但若采本文主张的规则，则新浪微博不得通过协议来排除脉脉获取用户信息的权利，否则本规则将在实践中被架空。

〔62〕 鉴于这涉及的是必要性原则的界定和适用问题，本文不作展开。值得一提的是，一审法院认定：“用户职业信息、教育信息具有较强的用户个人特色，不论对于新浪微博，还是脉脉软件，都不属于为程序运行和实现功能目的的必要信息”。需注意的是，法院此处所谓的“必要信息”，指新浪微博与脉脉订立的《开发者协议》中约定的“开发者可以为实现应用程序运行及功能实现目的之必要需求而收集相关用户数据”，与立法上要求的信息收集应遵循的“必要性原则”，未必一致。

〔63〕 天津市滨海新区人民法院已对上述三项行为发布了行为保全的裁决，参见（2019）津0116民初2091号民事裁定书。本文认为该裁决不当。

〔64〕 比如企业角度的数据可分为原生/衍生数据，而个人角度的信息可分为用户提供和非用户提供的信息（欧盟GDPR采取的分类方式）。

题。当然，我国《民法总则》第111条和第127条已将个人信息和数据区别对待，只不过或许是因为目前的数据法律问题争议较大而尚未在法律上明确数据规则。若是如此，通过个案性的司法裁判及“指导性案例”或典型案例等来逐渐厘清相关数据规则，或许是目前更为可行的选择。

其二，目前部分寄居于个人信息保护规则中的数据规则，也应作调整，比如区分不同的数据类型来设置相应的规则。目前我国已有众多涉及个人信息的规范性文件，比如，2019年4月公安部发布的《互联网个人信息安全保护指南》第6.6条“共享和转让”中规定“个人信息原则上不得共享、转让。如存在个人信息共享和转让行为时，应满足以下要求：a）共享和转让行为应经过合法性、必要性评估；……”该指南对数据共享的规则采取了不区分数据类型的一体对待的做法。但依本文的论证，在更新本指南时，或许可对不同类型的数据采取不同的规则。

结　　语

作为数字经济时代的核心资源之一，数据已成企业间的“兵家必争之地”。企业间的数据获取问题是目前司法实践中争议的焦点所在。数据获取规则的设计，将影响实践中商业模式的选择和相关产业的发展，同时也丰富了企业数据权益制度、不正当竞争制度等内容。

对企业数据获取规则，目前研究的主要思路在于，先界定企业对数据的权利属性及权利内容，从而得出企业间数据之争的行为边界。此类研究有着毋庸置疑的重要价值。但本文并非要加入此场“混战”中，而是转换思路，试图从获取数据是否需经企业和用户同意角度，去勾勒企业间的数据流动关系，希望能为未来属性问题上的“一锤定音”及相关司法裁判的改进提供智识上的积累。

Abstract　The Triple Authorization Principle, which was first raised in *Sina Weibo v. Maimai*, requires three authorization before a data collector collects data from a data holder: the Internet user's authorization to data holder, the Internet user's authorization to the data collector, and the data holder's authorization to the data collector. This principle should not be applied to all kinds of data. The basic rules of data collection among companies should be decided by the category of data: in the case of collecting identifiable and original data, the Internet user's rather than the data holder's consent is required; when collecting unidentifiable and derived data, the data holder's rather than the Internet user's consent is required; when it encounters to identifiable and derived data, both the Internet user and the data holder's consent are required; as for the unidentifiable and original data, the Internet user's consent is not required, and the data holder's consent is mandatory or not depends on whether the data is publicly available.

Keywords　Company's Data Rights, the Triple Authorization Principle, Original Data, Derived Data, Unfair Competition

（责任编辑：徐彦冰）