隐私政策在企业数据合规实践中的功能定位

李延舜

摘要：互联网企业往往通过隐私政策传达对消费者数据隐私的尊重，但一来很少有人点开并完整地阅读它，且面对给定的隐私政策无法讨价还价，二来消费者也难以判断隐私政策的合规性如何，三来政府监管机构能否以及如何对隐私政策进行执法尚不清晰，使得隐私政策并未发挥它应有的功能。实际上，隐私政策对内是企业治理规范，是企业积极主动地拥抱隐私、承担社会责任的体现，对外则是沟通消费者与企业数据处理行为的桥梁，是政府监管的重要内容。隐私政策文本不仅要体现法律遵从性，更要落实到企业数据合规实践中，在企业、政府、行业与消费者之间形成良性互动，搭建数字经济时代隐私保护的共同体。

关键词：隐私政策；数据合规；公司治理；社会责任

基金项目：河南省哲学社会科学规划项目“大数据企业数据合规机制研究”(2020BFX005)；司法部国家法治与法学理论研究一般项目“个人数据的法律保护研究”(17SFB2005)

中图分类号：D922.16　　**文献标识码：**A　　**文章编号：**1003-854X(2020)10-0136-09

数据合规对互联网企业影响甚巨：一是关乎主动还是被动面对法律风险。事先主动采取措施避免数据合规问题，通常比应对后续调查、负面舆论和诉讼风险低得多，且成本低廉；二是如果想成为行业领军企业，那必须考虑对法律规定和商业需求做更全面的评估；三是在与政府职能部门关系方面，要考虑企业面对多大的政府执法风险；四是在不同法域，要考虑不同程度和不同模式的数据保护法律，如欧盟和美国之间的消费者数据传输和共享。[①] 在数据合规实践中，隐私政策是一项特殊的存在。隐私政策是互联网企业向消费者发布的关于个人信息收集、存储、利用等行为的告知与解释性声明。除“隐私政策”外，“法律声明及隐私政策”、“隐私保护指引”、“用户服务协议及隐私保护政策”、“隐私权政策”、“个人信息保护政策”等皆代表相同涵义。隐私政策多以一个文本链接的形式存在，它像一把自带免责属性的尚方宝剑，为互联网企业数据合规保驾护航。早在 1997 年互联网发展初期，时任美国总统的克林顿就批准公布了《全球电子商务框架报告》，强调在保护互联网隐私方面，私营企业应当起到主导作用。这既与美国保护消费者隐私的模式交相呼应，也深刻反映出法律的特色——徒法不足以自行。数据保护立法再完美，其实现也要落实到企业的数据合规实践中，而这其中，隐私政策是重要一环。

一、隐私政策的属性分析

我们常在互联网企业网站或 APP 上发现“隐私政策”的链接。尽管少有人点开并完整的阅读它，它却在企业数据合规实践中承担越来越重要的角色，而这一“功能定位”要从其法律属性谈起。

(一) 告知与社会承诺属性

欧盟《一般数据保护条例》第 5 条第 1 款规定处理个人数据应遵循合法、合理和透明三原则，如果说合法性和合理性尚能做到有“迹”可循，那透

明性如何实现？答曰：以法定义务形式实现。基于巨大的知识与资本鸿沟，数据主体不可能主动获取详细透明的企业数据处理行为，企业需承担信息披露的法定义务。原因很简单，“与买方占有相关信息的情况相比，当卖方占有相关信息时，社会对信息披露义务的需求更强烈。”[②]唯有让公众知情，消费者才能放心地交由企业收集、处理其个人数据。不仅在欧洲，美国虽没有统一的数据保护法，但联邦贸易委员会却创制规则，要求企业提供在消费者看来有价值的信息，而不仅仅是禁止误导性说明。这种规则被称作“强制告知”，即使企业并没有被指控为虚假说明，它们仍有可能被要求执行强制告知。[③]在此意义上，隐私政策正是企业收集、利用个人数据“告知”义务的体现。

当然，告知并不仅仅是透明性原则的体现，它还与社会承诺相连。一方面，互联网经济是信任经济。2012 年，美国总统奥巴马发表的《网络环境下消费者数据隐私保护》工作报告指出：“信任对于维持网络技术给美国和世界其他国家带来的社会经济效益至关重要。正是基于消费者对互联网企业公平和负责任地处理个人信息的信任，消费者才选择在互联网上展示他们的活力、参与政治活动、建立和发展网络友情和从事商业活动。”[④]企业只有获取并维持市场上消费者的信任，才能继续在数字经济领域生存和发展。而经由隐私政策完成的“告知”正是获取消费者“信任”的最佳途径，同时，隐私政策也由“告知”形成“社会承诺”，因为只有承诺，才能赢得社会信任。另一方面，隐私政策的社会承诺属性还是企业社会责任的体现。社会责任是企业管理的一个基本要素，“企业管理者不像从前那样仅仅代表所有者的单方利益；他们越来越多地基于受托人角色行使职能，……今天，每家公司的高层主管不仅对股东负责，还对企业成员、消费者和公众负责。”[⑤]当越来越多的公众关注其数据隐私时，企业就必须对此作出回应，隐私政策也不再是纯粹的阅读文本，而是向功能文本转变。换言之，隐私政策就是企业向消费者作出保障其数据权利的社会承诺。即便消费者不怎么阅读隐私政策，隐私政策也成为监管机构、隐私权民权组织及社会媒体聚焦打量的重点。如果一个企业真心实意地遵守这些政策条款，那么可以得出结论：他们表现出了对公民隐私权的尊重。[⑥]

(二) 服务协议属性

随着隐私政策由单纯的“内容介绍型”向复合的“告知承诺型”转变，隐私政策的服务协议属性日益被学者们认可，国外如 Scott Killingsworth 认为企业隐私政策是网站与用户间的合同[⑦]，国内如谈咏梅等认为隐私政策“是建立在双方合意基础上的协议，是网络服务合同不可缺少的一部分”。[⑧]很多企业隐私政策文本上旗帜鲜明地表明了这一点，如《酷狗隐私政策》“本隐私政策为《酷狗用户服务协议》的重要组成部分”，《58 同城隐私政策》、《拼多多隐私权政策》证明文本中亦有相同或相似表述。司法实践也基本认可合同属性，如“卢星与小米科技有限责任公司网络购物合同纠纷”案中，法院就将小米隐私政策视为合同。[⑨]

这个判断在总体方向上没什么问题，但须注意以下四点：第一，隐私政策文本用语必须清晰直白、简洁易懂，充斥着法律术语且晦涩难懂的隐私政策文本不能简单认定为服务协议。如 2009 年初，Facebook 的律师团队对网站的保密条款做了他们认为很细微的变动，这些文件充斥着大量法律术语，他们认为用户几乎不会去认真阅读这些条款。但一些用户还是注意到了这些修订，并很快成立了一个“反对新服务条款者”的小组，成员达到 12 万。扎克伯格被迫取消新版本，并保证以后在制定网站相关文件时使用大家都能理解的语言，确保条款反映出用户的原则和价值[⑩]；第二，隐私政策不能泛泛而谈、空洞无物，隐私政策至少应当阐明数据收集的种类与目的、数据利用的限制以及数据主体的各项权利，否则难以认定其协议属性。如美国在一起涉及航空公司非法共享乘客信息的案件中，对其隐私政策的合同属性不予认可，理由是过于宽泛的声明并不构成合同条款[⑪]；第三，对隐私政策表示“理解”并“同意”的方式不同，也影响着隐私政策的合同属性认定。一般而言，网络上表达同意的情形分两种：点击生效 (明示) 和浏览生效 (默认)。[⑫]前者经由点击“我同意”或“我接受”按钮，而按钮又在文本的最下方，往往需要滑动页面，这个过程明确传达了“知情同意”的味道。而后者无论在程序上还是在实质上，都无法体现真正的“知情同意”，法院也会认为隐私政策仅仅是一份声明，而不具备协议属性[⑬]；第四，理想中的隐私政策与用户服务协议并不冲突，但现实中有很多例外情形，如《小米商城隐私政策》就规定，“如果您同意了适用的用户协议，并且此类用户协议和本隐私政策之间存在不一致，将以此类用户协议为准”。还有一些巨型网络公司如百度、腾讯，往往有一个总的隐私政策和各产品/服务的单行隐私政策，此时，各产品的隐私政策多优先适用。当然，企业对

隐私政策和用户协议效力大小的自行认定并不一定就是最终结果，但从法理上讲，“有利于数据主体保护的条款优先”。[14]

(三) 公司治理规范

成熟的大型公司有一个特点，它们有能力拥有“政治和专门制定政策的机构，使它们摆脱日常运营中的真实难题，从足够长远的角度看待问题，并考虑到组织与社会的关系。”[15] 企业的隐私官员 (或法律总顾问) 必须参与到公司制定战略决策的过程中去，如果没有，那这个企业就是在自寻烦恼。没有人会为隐私付费，这曾经是真的，但情况正在发生变化。2000 年的一项研究发现，如果消费者觉得自己的隐私受到了保护，他们每年会增加 60 亿美元的互联网消费。[16] 来自卡内基·梅隆大学的研究结果也表明，隐私很可能成为数字时代企业的一项重要竞争优势：“与认为消费者不大可能为隐私付费的常规观点相反，消费者可能会愿意支付额外费用来保护隐私。我们的研究结果还表明，那些运用技术手段展现其正面隐私政策态度的企业可能会由此获得竞争优势。”[17] 可见，消费者面对日益严重的隐私危机，他们已经做好准备为隐私付费。“棱镜门”爆发后，原先名不见经传的网络搜索引擎 DuckDuckGo 瞬间爆红，搜索量增长达 30%以上，其卖点正是“从不追踪用户”且“从不过滤信息”。虽然搜索结果针对性方面有所欠缺，却赢得了诸多隐私敏感用户的支持。

隐私政策对外是沟通消费者信任与达成协议的桥梁，对内则是公司治理的重要规范。首先，隐私政策是企业合规风险评估的重要指标。“成功的隐私保护不是通过证明他人享有统治权和同意权来衡量的，而是在实际生活中预防实质损害，例如，防止数据泄露，以让人信赖的方式保护那些处于岌岌可危状态的信息。……此外，此种做法已经将隐私从一个遵循法规的活动转向风险评估的步骤，要求企业在做出有关产品设计、市场准入和政策发展的决策时嵌入隐私。”[18] 在网络与数字经济情境中谈隐私保护，必然要求企业拥有一个动态的、前瞻性的隐私展望：它不仅仅是法令和规章，而越来越成为企业发展风险管理实践的一部分。其次，隐私政策督促企业自产品/服务设计之初就嵌入隐私。该理念最早由加拿大信息及隐私专员安·卡沃基安提出，并逐渐成为美国联邦贸易委员会倡导的商业及政策制定框架的基础。[19] 企业层面的决策是避免隐私受到侵害的最佳途径，就此而言，隐私保护是一段旅程而不是终点，隐私讨论必须要从合规办公室转移至整个公司开发新产品和服务的过程中。[20] 迈阿密大学迈克尔·弗鲁姆金教授提出一个有趣的想法：要求政府和大数据依托企业仿照环境影响报告，拟定隐私影响条款。这既有助于告知公众数据收集的内容和原因、数据存储和使用的方式，也会鼓励决策者在任何项目开发的早期阶段就考虑隐私的问题。[21] 再次，隐私政策还可能是企业进行数据跨境转移、拓展国际业务的必备要件。2016 年，欧美就个人数据跨境转移达成“欧盟—美国隐私盾”协议，相比之前的安全港协议，其进步之处在于企业需承担更强义务。美国企业一旦提交加入隐私盾的申请和确认书，就应当完全遵守其中的各项隐私原则，公开企业隐私政策，接受美国商务部、联邦贸易委员会等有权部门的监督和执法。[22] 可见，数据保护水平相对较低地区的大数据企业要想走出国门，离不开完善且合规的隐私政策。

(四) 行业自律规范

从发展历程看，市场对消费者个人数据的态度呈现出一个由无视到尊重、由恣意到规制、由混乱到有序的过程，在这个过程中，行业自律占据重要地位。大数据时代，消费者数据资源的挖掘与利用成为数据经济发展的“石油”，但这一过程不能以公民隐私为代价。面对法律越发严格限制的威胁时，各行业往往会承诺进行自我监管。原因有二：其一，市场的特殊地位。市场既是消费者数据隐私的潜在威胁者，又是数据保护的前沿实践者。早有学者指出：“非官方手段在保护个人隐私方面往往更加高效、敏感。这一点在保护隐私权的具体例子中已得到证实——通过科技手段、市场、行业自律、企业竞争以及个人判断，人们可以获得相当周全的隐私权保护。”[23] 其二，行业自律可降低企业生存与发展中的风险。企业决定自律可能会因为担心消费者的抵制，更可能是出于担心政府的规制比自我约束更加繁重。美国联邦贸易委员会曾于 1998 年公布了一个调查报告，认为有必要进行正式立法以确保互联网隐私得到保护，并提出了立法构想。但该意见遭到美国企业界的强烈反对，他们强调到 2000 年，美国制定隐私政策的网站已经增加到 90%，这说明情况比联邦贸易委员会进行调查时已得到极大的改善。当然，企业界也深知网站自我规范的实现是一个问题，可行的办法就是成立自律组织，对网站隐私政策进行必要监督。2008 年，世界上一些主要的网络公司签署了《全球网络倡议》，它要求签署公司和其他组织“遵守并保护用户对言论自由和隐私的权利”。[24] 2012 年，我国百度、奇

虎360、腾讯等12家搜索引擎企业在北京签署了《互联网搜索引擎服务自律公约》，声明搜索企业有义务保护用户隐私和个人信息安全。

制定隐私规则是行业自律的主要措施，而这些规则又要求互联网企业发布并遵守隐私政策。如美国直销协会、在线隐私联盟和网络广告促进会等皆为其成员制定隐私规则或隐私指引，要求成员企业发布并遵守隐私政策。网站必须全面告知消费者关于个人数据处理的行为，包括数据收集的种类、用途、存储期限以及是否与第三方共享、转移等等。对这些团体而言，自律意味着有一个明确的隐私政策，并在企业进行初次或二次三次个人数据处理时，给消费者提供选择性退出的机会。[25] 通过对国内一些互联网企业隐私政策文本的阅读发现，隐私政策与产品/服务、场景的结合越来越紧密，如在线购物类的隐私政策比较接近、社交交友类的隐私政策也相对趋同，这一方面表明隐私政策呈现类型化、个性化、定制化的趋势，也表明自律规范正在潜移默化地影响着企业数据处理行为。

二、隐私政策是企业数据合规从文本到实践的连接点

隐私之于信息经济，如同消费者权益保护和环境问题之于20世纪的工业社会。[26] 可见，隐私正是信息社会“木桶理论”中的那块“短板”，互联网经济的规模、效益，将最终取决于消费者的隐私保护水平。那么，作为普通消费者唯一能接触到的隐私政策，在互联网经济中又处于什么地位，或者说，承担何种功能呢？

(一) 数据隐私法要贯彻到隐私政策文本中

网络环境下，法律和技术对消费者数据保护都有着重要作用。但“与通过法律界定信息收集者与信息提供者权利义务关系的调整方式相比，在法律上强制性要求技术措施在设计上必须包含信息隐私保护的技术效果将是一个更直接、更有效的方法。”[27] 换句话说，法律塑造特定的隐私实践，它们构成了隐私方法的“起点”，或者是隐私三角形的“底边”。关注消费者隐私，首先应关注隐私实践的法律遵从性问题。如果将隐私政策视为一种具体隐私实践的话，那首先要做的，就是将数据保护法中的义务性规范贯彻到隐私政策文本中。通过对美国和欧盟的互联网经济政策和数据保护法进行梳理，也能发现这个趋势。

先看美国。2010年奥巴马政府发布《总统的隐私蓝图》和《消费者隐私权人权法案》，由商务部推动的互联网政策任务组，负责协调各政府机构，全面审查其描述的“在隐私政策、版权、全球自由信息流动、网络安全和互联网经济中的创新之间的关系”。[28] 2011年《商业隐私权利法案》力图“公平协调处理保护消费者免遭未经授权的跟踪和允许企业机动灵活地提供新的服务和技术这二者之间的矛盾冲突。在该法案约束之下，公司必须依法对其收集和使用私人信息的途径和方法做清晰表述，同时向消费者提供选择性拒绝任何未经授权的信息收集行为之权限。”[29] 2012年2月，奥巴马又签署白宫发布的工作报告《网络环境下消费者数据隐私保护》，介绍消费者隐私权利法案七项原则的同时，敦促多方利益主体参与推动，尽快形成执行细则。《儿童网络隐私保护法》更进一步，明确规定了面向家长的网站隐私声明中必须具备的要素，其目的在于避免出现那种不容讨价还价的隐私声明和用户同意。通过指出可接受的隐私声明的主要框架，该法踏出了解决信息不对称问题的第一步。[30] 2018年美国《加州消费者隐私法案》不仅规定企业在线收集加州消费者数据前，必须先发布网站隐私声明，而且详列了企业应当主动披露的事项和应消费者要求应当披露的事项。

再看欧盟。《一般数据保护条例》两个条款与企业隐私政策息息相关：第12条是基于数据处理的透明性原则，要求企业用“简洁、透明、易懂和易于获取”的书面形式，以清晰和直白的语言，向数据主体提供详细的隐私通知，披露数据控制者的身份和联系方式、数据保护官的联系方式、数据处理目的、数据处理法律依据、数据控制者或第三方的正当利益、数据接收者的类型、数据存储期限、数据主体权利等；第47条则指向有约束力的公司规则，其性质与公司隐私政策等同，可视为有效服务协议的组成部分。除明确赋予数据主体可执行的数据权利外，有约束力的公司规则应当至少明确：企业集团或其他经济主体及其联系方式、有关数据转移的规定、规则的法律约束效力、对一般数据保护原则的适用、责任承担及免除情形、如何将公司规则提供给数据主体、数据保护官的任务、申诉程序、公司内部如何实现对规则的遵守等等。

除互联网经济政策和数据保护法试图将其精神和义务性规范贯彻到企业隐私政策外，数据保护或执法机构也不断推进隐私政策的完善。如美国联邦贸易委员会很早就根据反不正当竞争法理论敦促企业发布网站隐私声明，而如果企业未能遵守自身的

通知、规程和声明，在大多数情况下会因为违反包括反不正当竞争法和侵权法 (虚假陈述) 在内的多种法律而遭受处罚。[31] 美国商务部也不甘落后，在1998 年发布的《隐私权保护的有效自律规范》草案中，强调为保证自律规范的实施效果，监管部门有权验证企业在实践方面是否遵守隐私政策。如果企业不执行隐私政策，则应承担相应后果。[32] 2010 年又发布了题为“网络经济中的商业数据隐私与创新：一个动态的政策框架”的隐私报告，该框架的可取之处包括：重构“公平市场信息实践原则”，行业隐私政策的标准化，成立直接与联邦贸易委员会展开合作的隐私政策办公室，……等等。[33]

问题探讨到这里，不禁要问：即使将对政策和法律的遵从性内化进企业的隐私政策中，隐私政策真的能发挥其规制企业数据处理行为的功效吗？毕竟，几乎没有人有时间、精力或者决心浏览一遍各不相同的隐私政策。更尖刻的评论指出：“只有在臆想的世界中用户才真正阅读这些通知的内容并在表明其同意之前真的理解其含义。‘通知和同意’在服务者和用户之间形成了一个不平等的有关隐私的谈判平台。……这是一种市场失效。”[34] 的确，隐私政策在发挥其“告知与同意”的功能上效果大打折扣，但万不可忘记，企业隐私政策还有其“规范”功能，还能因其承诺属性和合同属性成为监管机构的执法对象——“除了法律可能具有的规定之外，它们还设定了商业使用数据的界限，根据消费者保护法规确定了可实施的法律责任。它们对信息披露的要求可以迫使公司对它们的隐私实践进行评估，并在其对消费者信息的处理中强调纪律。”[35] 换言之，企业绝不会因发布隐私政策就自动获得了数据处理的正当性，这仅仅是一个开始，隐私政策也绝不是一份束之高阁的宣示性材料，而是企业数据合规从文本到实践的连接点。

(二) 隐私政策终要落实到企业隐私实践中

“从设计着手隐私”理论“把隐私看作一个商业问题而不是依从性问题，达到隐私保护和承诺功能的双赢”。[36] 互联网企业拥抱大数据时代的正确姿势绝非眼中只有数据收集和挖掘利用，而是要把隐私看作默认需求，主动而非被动地将隐私嵌入到产品/服务设计中，实现数字经济和隐私保护的正和博弈。而在此过程中，出台并将隐私政策落实到企业隐私实践中去是至关重要的一步。

1. 隐私官员职业化

隐私官员职业化是企业数据合规实践的第一步，称呼或职能部门设置上可能有所不同，有的直接由法务部或其他部门人员兼任。世界范围内，德国是首个引入数据保护官概念的国家，旨在通过企业自我任命的隐私保护者来推进企业的自我监督，从 20 世纪 70 年代起，企业就负有法定义务任命数据保护官。在国内而言，360 公司是国内首家设置首席隐私官 (CPO) 的大型互联网企业，CPO 负责处理 360 软件产品可能涉及到用户个人信息的各项事务，包括规划和制定公司的隐私政策、审核各产品的用户使用协议、监督各产品的工作原理和信息处理机制等。

欧盟《一般数据保护条例》第 37 条规定了数据控制者或处理者“应当”或“可以”委任数据保护官的情形，并在第 38 条规定了数据保护官的职位保障。隐私官员职业化的重要性在于，他们可以向不同的外部利益相关者传输消费者隐私期待的力量，并且作为企业和外部利益相关者“最佳实践方式”的联系桥梁，这一点可以通过《一般数据保护条例》第 39 条“数据保护官的任务”体现出来。数据保护官不仅对企业数据处理行为进行隐私风险评估、职员隐私保护意识和岗位培训、制定并监督遵守隐私政策，还要与监管机构进行合作，充当监管机构的联系人。可见，数据保护官职位虽为企业所设，其职责或者说利益指向并不是“一切为了企业”，而是充当监管机构、企业以及消费者三方的协调、联络角色。当然，企业最初设立隐私官员的初衷是复杂的，有的是为了遵守法律，有的是为了树立标杆形象，但不管怎样，“结构决定功能”，“如果能够从结构上构筑信息控制者积极主动作为的组织体系，就完全有可能改变其行为方式，使个人信息保护成为其内生机制的一部分。”[37] 隐私官员的职业化会逐渐释放其“结构性”红利，随着设置隐私官员的企业数量的增加，我们看到用户隐私在企业的生存和发展中占据日益重要的地位。隐私官员也开始有了自己的组织，即国际隐私专家协会。

2. 隐私政策标准化和技术化

面对形形色色的各类企业隐私政策，有心人会思考有没有“标准版”的隐私政策呢？如果有，那消费者就不必担心因无心看冗长的隐私政策而错过了自己的最佳选择。原因很简单，“消费者一般都欢迎标准：他们不必面对本想选择胜利者却选择了失败者的风险。在单一的网络或无缝互联的网络中，他们可以享受最大的网络效应。”[38] 隐私政策是否可以标准化呢？答案是能也不能。说“不能”是因为互联网企业所提供的产品 / 服务千差万别，所需收集和使用的数据类型也各有不同，自然做不到

隐私政策的标准化；而说“能”则基于数据保护原则的同质以及隐私政策文本结构的趋同，这更多地体现为一个技术问题。

还有另外一种理解隐私政策标准化的思路，是与隐私政策贯彻落实的技术化联系在一起的。原理如下：政府要求企业张贴隐私政策，但是，并不是每位用户都会阅读这些隐私政策，即使阅读了，用户又能记住多少企业的隐私政策呢？你能清楚地分辨提供不同产品/服务的企业所提供的隐私政策有何区别吗？在这里，政府忽略了一件事，它没有要求隐私政策应当为计算机所识别。而一旦隐私政策可以被计算机所识别，那发展 P3P 的前景就光明了。P3P (Platform of Privacy Preferences Project) 又称为隐私偏好平台项目，由万维网联盟开发，能将用户偏好与网站隐私政策进行比对。P3P 协议包括引导浏览器的规则，引导浏览器读取和解析网站的隐私政策，同时，用户的偏好将被嵌入浏览器，这样，P3P 只允许用户在与其偏好一致的网站上提供个人数据。当用户进入数据收集范围超出其意愿提供的信息范围的网站时，或进入拥有让用户感到不适的隐私政策的网站时，浏览器将会向用户提供警告。[39] 换句话讲，网站通过 P3P 协议提交一个请求，我们将其视为有约束力的要约。如果用户接受了该要约，则合同成立。[40] 可见，P3P 最大的好处就是推动隐私政策的简化和标准化，因为隐私政策必须以机器可读格式存储，而不能用晦涩难懂的法律术语来表达。[41] 当然，P3P 也不是万能钥匙，它无法保证隐私政策的执行，也无权追查那些故意违背隐私政策的企业。但不管怎样，P3P 代表了一代试图通过技术手段让用户披露自己个人信息的控制能力与网站隐私政策共生的努力，随着 P3P 这样的互联网技术架构进一步成熟，更有可能在消费者隐私保护和经济效率之间达致平衡。

3. 隐私政策问责制

当前，整个数据保护法或者说隐私规范的重心正在转向问责，“知情与同意”模式仅有助于数据初次收集的“合法化”，但数据资源的价值多体现在二级用途上。所以，我们需要设立一个不一样的隐私保护模式，这个模式应该更着重于数据使用者为其行为承担责任，而不是将重心放在收集数据之初取得个人同意上。[42] 再则，将责任从民众转移到数据控制者也存在充足的理由，因为数据控制者比民众更明白如何利用数据以及从中受益。

在企业数据合规的问责体系中，隐私政策地位凸显。政府“怀疑”与“巡视”的目光常聚焦于企业隐私政策，企业数据处理行为的合规性论证也“求助”于隐私政策，消费者数据安全与隐私保护的诉求也仰赖于隐私政策，如此，政府、企业与消费者不约而同地将视线转向隐私政策。以数据安全为例，之前企业可能不太会斥巨资、花大力气来研发、改进数据安全防护技术、认证安全保护等级、制定安全事件应急预案，但一旦让企业为数据泄露负责，结果可能会向好的方向发展。企业在大规模信息泄露事件中固然是受害者，但绝不是无辜的受害者，真正无辜受害的是消费者。2017 年 Uber 数据泄露事件中，5000 万乘客的姓名、电邮和电话被盗；同年美国知名信用机构 Equifax 遭到黑客攻击，大约 1.43 亿用户敏感信息泄露；2018 年 Facebook 发生数据泄露丑闻，超 8700 万用户信息外泄。一系列安全事件中，企业存在过错 (至少是重大过失) 的情形比比皆是，比如 Uber 曾经花 10 万美元向黑客买封口费，Facebook 授权政治数据分析公司 Cambridge Analytica 收集用户信息。2017 年国内暗网市场知名供应商双旗抛售 10 亿条从中国互联网巨头盗取的大量数据 (包括网易、腾讯控股、TOM 集团、新浪、搜狐公司等)，有些数据是明文呈现，有些是很容易就能破解的 MD5 散列值。可见，企业并没有重视数据安全保护，而这就是企业承担责任的原罪。之前，大规模数据泄露所需要付出的代价，都由数据被泄露的人承担了，在经济学上，这被称为外在性 (Externality)：某个决定的后果不由决策人承担。外在性限制了公司提升自身安全性的动力。[43] 现在，是时候通过提高数据泄露的成本，让企业花费更多力气去保护消费者的数据隐私了。

三、面向企业隐私政策的执法

通过隐私政策实现数据合规离不开“面向企业隐私政策的执法”，因为市场的天性是逐利，你不可能让一个“利润至上”的企业自缚手脚。

(一) 对隐私政策进行执法的必要性

互联网企业可能会引用“买者自负”原则，声明用户自愿签署这种浮士德式交易。隐私政策文本中也存在诸多免责条款，如《酷狗隐私政策》7.5 条就列明四种情形下酷狗不承担任何责任。但问题在于，不管隐私政策文本中列明的免责条款合法性及合理性有多少，企业对自身处理消费者个人数据的行为要负起责任来。换句话讲，企业主一直强调的“知情同意”并不是所有数据处理行为的免责金牌。一直被诟病的用户服务协议之“格式合同”属

性在消费者与企业资源与能力上的巨大差异面前尽览无疑。梅迪库斯讲过，“私法自治作为一种形式上的人人平等的自由，没有顾及到实际上并非人人平等的事实。人与人之间在财产、体能和精神能力，在市场地位和掌握信息以及在其他许多方面，到处都存在着差异。”[44] 人与人之间尚且如此，更何况人与企业。无论对隐私政策赋予何种属性以规范企业的数据处理行为，消费者点击同意隐私政策的过程都是在一个双方地位不对等的平台上。

隐私已经成为数字经济良性、健康发展的重大挑战，隐私问题得不到解决，数字经济的高楼大厦终归建基于砂砾之上。对隐私政策进行执法，是当前可行的重要数据保护实践路径。一方面，数据(个人信息) 保护法迟迟未能出台，个人面对无处不在的数据收集与处理又无能为力，只有将希冀的目光转向企业及其隐私政策。即使相关法律出台，其最终落实还是要看企业的数据合规实践。再者，有远见的企业高管也愿意将数据合规打造成品牌或荣誉，成为新的客户增长点。在这其中，隐私政策作为沟通企业与消费者的隐私桥梁，对双方都有特别的意义。对消费者而言，隐私政策是目前可见的、能接触到的数据保护的最重要一根稻草，淳朴的消费者认为隐私政策体现出了企业对消费者的尊重；对企业而言，隐私政策不仅是数据合规的需要，更是战略发展的需要，消费者所需即企业改进的方向。另一方面，隐私政策公布后，企业会认真遵循吗？企业的天性是逐利，而消费者数据将是决定未来谁能成为赢家的决定性因素，所以企业绝不会放过任何能获取到的数据。事实也确实如此，斯坦福大学主持的一项研究发现，“在 64 家作为研究对象的拥有线上广告业务的公司 (包括谷歌、雅虎、美国在线和微软) 中，有一半在持续开展数字跟踪活动，即便对象用户已经点选了不被跟踪选项。因此，即使用户已经就隐私问题积极主动地采取了前摄性措施，也不代表那些收集者们针对用户的信息收集行为就将被真正阻止。”[45] 原因很简单，单纯依靠自由市场机制来扭转隐私侵害的趋势是不太可能的，“在控制掠夺性收集信息的问题上，信息商品交易的回报和营销利润太高，单纯依靠市场的力量难以实现这种控制。”[46] 所以，必须在自由市场之外，有强有力的政府监管介入，以纠正当前隐私保护市场的失灵。

莱斯格教授认为，真正有效社会规范的前提条件是，“社会规范的实施群体必须包括那些被规制行为的成本负担者。换句话说，建立社会规范进行自我规制的行业并不承担使用所获信息的成本。成本——消费者的隐私是由个体而非公司来承担的，而消费者并不是社会规范的制定者。”[47] 斯皮内洛也指出，企业间的“数据销售或交换给数据主体强加了一个成本：出售他或她的信息导致隐私的丧失。这一成本不是由交易双方来承担，而是由数据主体不情愿地承担了。”[48] 如何改变这种默认规则，让企业真正担负起数据处理行为的责任来，唯有依靠隐私政策从文本到实践功能的转变。隐私政策绝不是企业逃避合规义务的盾牌，而是企业承担数据保护社会承诺、社会责任的体现，是消费者寻求隐私保护的信赖规范，从而，隐私政策毫无疑问应成为数据合规实践中监管机构的重要执法对象。

(二) 对隐私政策进行执法的类型

对隐私政策进行执法的类型主要有两种：一是对企业的数据处理行为是否符合企业发布的隐私政策进行执法；二是对企业发布的隐私政策是否合乎数据 (隐私) 保护法进行执法。

先看第一种。美国 Toysmart 公司是一家从事网上销售幼教玩具的公司，其隐私政策曾承诺：“您可以放心，您的信息永远不会与第三方共享”。然而天有不测风云，公司倒闭了。在破产清算程序中，Toysmart 公司打算出售它的消费者信息。该事件引发了隐私倡导者的强烈批评，美国联邦贸易委员会也起诉该公司违背隐私承诺，是一种不公平、欺诈行为。[49] 后来，Toysmart 公司与联邦贸易委员会达成和解协议：禁止 Toysmart 公司将消费者个人信息作为资产单独出售；Toysmart 只能将公司与消费者信息打包出售给有资格的买家；有资格的买家必须遵守 Toysmart 之前制定的隐私声明，如果要改变信息收集和使用方式的话必须事先征求消费者的明示同意。谷歌和 Facebook 也先后遭遇过类似的执法。2010 年 2 月，谷歌推出一项社交服务 (Google Buzz)，Buzz 推出的当天，Gmail 用户就收到邮件劝说他们使用新服务，并给予两个选项“看看 Buzz”和“不，去我的收件箱”。然而，即便选择了后者的用户仍然被纳入了其社交网络之中，选择了“看看 Buzz”的用户也并未被明确告知：他们邮件中的常用联系人名单将会默认公开出现在 Buzz 社交网络中。该服务引发了谷歌用户的大量投诉，而当时谷歌的隐私政策声称：“当您使用一项需要注册的服务时，我们会要求您提供个人信息。如果我们以不同于收集时的目的使用这些信息，我们会在使用之前征求您的同意”。Facebook 也曾因未能遵守隐私政策而遭到联邦贸易委员会的起诉，联邦贸易委员

会列举了一些 Facebook 违背其隐私政策的事例，如 Facebook 曾更改网站设置，将原本设置为私人信息的内容改为公开，却未曾告知消费者，也没有事先获得授权。对上述事件分析可见，美国联邦贸易委员会执法的依据正是互联网企业自身发布的隐私政策。根据《联邦贸易委员会法》第五条，联邦贸易委员会有禁止不公平和欺诈性商业行为的职权，联邦贸易委员会正是通过对该条的充分解释和援引，对企业隐私政策进行执法。在具体案件中，“被认为是具有误导性或欺骗性的行为包括错误的口头或书面表述，误导性的报价，未经充分披露而出售有风险或系统缺陷的产品，未披露传销信息，使用引诱和转换的方法，未履行所承诺的服务，未实现担保义务”，都被认为是对第五条的违反。[50]

再看第二种。如果将第一种视为企业遵循所承诺规范的话，那第二种就是对所遵循的规范的合法性进行审查。欧美基于不同的数据保护模式，对这两种执法类型各有侧重。美国以分散立法和行业自律为主的消费者隐私保护模式更侧重于第一种类型的执法，因为来自同业成员和市场的巨大竞争压力使得企业大多数情况下信守承诺；相比之下，采取统一立法模式的欧盟更侧重于第二种执法。如西班牙与法国的企业很大程度上将隐私职能作为遵守确定的法律命令，哪怕自己怀疑做不到也要严格执行。[51] 在此理念下，企业遵守隐私政策是企业数据合规实践的应有之意，而在此之前，隐私政策首先要合规。所以，面对谷歌 2012 年更新隐私政策，将 60 余种产品/服务的隐私政策打通之事件，欧盟和美国表现极为不同。美国联邦贸易委员会不仅未对谷歌的新隐私政策作出处罚，加利福尼亚州的联邦地方法院甚至在隐私组织 EPIC 对联邦贸易委员会的不作为告上法庭的案件中作出裁决：虽然法院承认谷歌改变隐私政策给消费者隐私带来的问题的严重性，但法院没有权力强制联邦贸易委员会进行执法。[52] 但在欧洲，情况却截然不同，西班牙、英国、德国、意大利、法国、荷兰等国都对谷歌新隐私政策展开调查。据英国《卫报》网站 2013 年 12 月 20 日报道，西班牙隐私监察委员会对谷歌在未提前告知用户、未给出合理理由、未取得用户同意的前提下，将不同在线服务的隐私政策进行整合从而获取用户个人信息的行为作出 90 万欧元的处罚。据英国路透社 2014 年 1 月 8 日报道，法国国家信息自由委员会对谷歌罚款 15 万欧元，其理由是：谷歌将 60 款隐私政策打通的行为，并未给用户提供退出此方案的选项，并且谷歌也没有向法国用户充分告知个人数据被处理的情况，也未明确告知处理这些数据的目的。更严重的处罚发生在《一般数据保护条例》生效后的 2019 年 1 月 21 日，法国国家信息自由委员会向谷歌开出了 5000 万欧元的罚款。其理由是：谷歌在两个方面违反了《一般数据保护条例》，一是未满足透明度和信息相关要求 (数据最小化)，二是没有为其数据处理流程获得法律依据。在涉及隐私政策部分，法国国家信息自由委员会指出，用户许可不够具体，因为谷歌要求必须完全同意隐私政策中的服务条款和数据处理条款，而非区分各种不同目的 (如个性化广告或语音识别等) 来同意各项条款。

需要指出的是，欧盟与美国关于前述两种类型的执法侧重只是相对而言，随着数据国际传输和保护的趋势增强，两种执法模式可能都会出现。比如欧盟与美国达成的隐私盾项目，美国商务部会审核申请加入该项目企业提交的加入申请和隐私声明，包括隐私声明是否与隐私盾原则相悖，欧洲数据保护机关可以要求企业履行合规义务，民事原告可以把企业告到法院。[53] 尽管隐私盾协议已于 2020 年 7 月 16 日被欧盟法院认定无效 (用于保护数据隐私的标准格式条款仍合法)，但相信在美国与欧盟开启讨论、筹备的新制度中，隐私政策仍是数据监管的重要对象。从本质上讲，对企业隐私政策的执法与数据 (隐私) 保护的政府监管是一脉相承的，前者是后者的重要组成部分。在数据合规实践中，我们必须对企业经营有明确的态度，制定一套被广泛接受的标准让企业遵守，不能让企业将自己视为自身社会责任的唯一裁决人。

注释：

①㉛㊸ 参见 [美] 狄乐达：《数据隐私法实务指南——以跨国公司合规为视角》，何广越译，法律出版社 2018 年版，第 14—15、21、29 页。

② [美] 斯蒂文·沙维尔：《法律经济分析的基础理论》，赵海怡等译，中国人民大学出版社 2012 年版，第 302 页。

③ [美] 理查德·A. 波斯纳：《法律的经济分析》，蒋兆康译，法律出版社 2012 年版，第 546 页。

④ 周辉等：《网络环境下消费者数据的隐私保护——在全球数字经济背景下保护隐私和促进创新的政策框架》，《网络法律评论》2013 年第 1 期。

⑤⑮ [美] 霍华德·R.鲍恩：《商人的社会责任》，肖红军等译，经济管理出版社 2015 年版，第 53、53 页。

⑥㉕㊻㊽ [美] 理查德·斯皮内洛：《铁笼，还是乌托邦——网络空间的道德与法律》，李伦等译，北京大学出版社 2007 年版，第 148、145、145、145 页。

⑦ Scott Killingsworth, Minding Your Own Business: Privacy Policies in Principle and in Practice, Journal of Intellectual Property Law, 1999, 7(57).

⑧ 谈咏梅、钱小平：《我国网站隐私保护政策完善之建议》，《现代情报》2006年第1期。

⑨ 参见甘肃省天水市中级人民法院 (2016) 甘05民终第427号民事判决书。

⑩㉔ [美] 拉里·唐斯：《颠覆定律：指数级增长时代的新规则》，刘睿译，浙江人民出版社2014年版，第18、101页。

⑪ See Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196, 1200 (D. N. D. 2004).

⑫ See Deborah Davis Boykin, Survey of E-Contracting Cases: Browsewrap, Clickwrap, and Modified Clickwrap Agreements, Business Lawyer (ABA), 2012, 257(68).

⑬ 高秦伟：《个人信息保护中的企业隐私政策及政府规制》，《法商研究》2019年第2期。

⑭ 王融：《大数据时代：数据保护与流动规则》，人民邮电出版社2017年版，第73页。

⑯ 转引自 [美] 布鲁斯·施奈尔：《数据与监控——信息安全的隐形之战》，李先奇、黎秋玲译，金城出版社2018年版，第187—188页。

⑰ Janice Y. Tsai, Serge Egelamn, Lorrie Cranor, Alessandro Acquisti, the Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, Information Systems Research, 2011, 2(22).

⑱⑳ [美] 肯尼斯·A.班贝格、迪尔德丽·K.穆丽根：《书本上的隐私和实践中的隐私》，魏凌译，载张民安主编《隐私权的性质和功能》，中山大学出版社2018年版，第253、269页。

⑲ See Stuart L. Pardau&Blake Edwards, The FTC, the Unfairness Doctrine, and Privacy by Design: New Legal Frontiers in Cybersecurity, Journal of Business and Technology Law, 2017, 227(12).

㉑ Michael Froomkin, Regulating Mass Surveillance As Privacy Pollution: Learning From Environmental Impact Statements, University of Illinois Law Review, 2015, 1713.

㉒ 参见中国信息通信研究院互联网法律研究中心、腾信研究院法律研究中心：《网络空间法治化的全球视野与中国实践》，法律出版社2016年版，第279页。

㉓ 张民安：《公开他人私人事务的隐私侵权》，中山大学出版社2012年版，第527页。

㉖ Quoted in James Gleick, Big Brother Is Us, New York Times, September 29, 1996.

㉗ Julie E. Cohen, DRM and Privacy, Berkeley Technology Law Journal, 2003, 609(18).

㉘ 转引自 [美] 达尔·尼夫：《数字经济2.0：引爆大数据生态红利》，大数据文摘翻译组译，中国人民大学出版社2018年版，第206页。

㉙ Gautham Nagesh, Kerry and McCain Throw Their Weight Behind Privacy Bill of Rights, Hillicon Valley, April 12, 2011.

㉚ [美] 保罗·M·施瓦茨：《网络隐私权和国家》，廖嘉娴译，载张民安主编《公开他人私人事务的隐私侵权》，中山大学出版社2012年版，第506—508页。

㉜㊼㊾㊷ 参见汪靖：《不被洞察的权利——互联网精准广告与消费者隐私保护研究》，复旦大学出版社2016年版，第143、19、175、185—186页。

㉝㊺ 参见 [美] 特伦斯·克雷格等：《大数据与隐私——利益博弈者、监管者和利益相关者》，赵亮、武青译，东北大学出版社2016年版，第33、55—56页。

㉞ 参见吴伟光：《大数据技术下个人数据信息私权保护论批判》，《政治与法律》2016年第7期。

㉟ [美] 马克·罗滕伯格等主编：《无处安放的互联网隐私》，苗森译，中国人民大学出版社2017年版，第170—171页。

㊱ 刘雅辉等：《大数据时代的个人隐私保护》，《计算机研究与发展》2015年第1期。

㊲㊶ 周汉华：《探索激励相容的个人数据治理之道——中国个人信息保护法的立法方向》，《法学研究》2018年第2期。

㊳ [美] 卡尔·夏皮罗、 [美] 哈尔·R.范里安：《信息规则：网络经济的策略指导》，孟昭莉、牛露晴译，中国人民大学出版社2017年版，第190页。

㊴ Simpson, G.R., the Battle Over Web Privacy, The Wall Street Journal, March 21, 2001.

㊵ William McGeveran, Programmed Privacy Promises: P3P and Web Privacy Law, New York University Law Review, 2001, 76.

㊶ [德] Christopher Kuner：《欧洲数据保护法——公司遵守与管制》，旷野、杨会永等译，法律出版社2008年版，第42页。

㊷ [英] 维克托·迈尔—舍恩伯格、肯尼思·库克耶：《大数据时代：生活、工作与思维的大变革》，盛杨燕、周涛译，浙江人民出版社2013年版，第220页。

㊸ [美] 布鲁斯·施奈尔：《数据与监控——信息安全的隐形之战》，李先奇、黎秋玲译，金城出版社2018年版，第288页。

㊹ [德] 迪特尔·梅迪库斯：《德国民法总论》，邵建东译，法律出版社2013年版，第144页。

㊿ Daniel. J. Solove & Woodrow Hartzog, The FTC and the New Common Law of Privacy, Columbia Law Review, 2014, 583(114).

作者简介：李延舜，河南大学法学院副教授，河南开封，475001。

(责任编辑　李　涛)