如何设计一部隐私法*

朱莉·科恩　著**

李汶锴　张月明　译***

一、引言

在经历多年失败后,对美国信息隐私立法提案的审议终于开始在国会两院推进了。在最近结束的第 116 届国会上,引人注目的提案众多,但无一脱颖而出。随着第 117 届国会的开幕,对于如何设计一部成功的隐私法,华盛顿的政策制定者正在形成更多新的共识。本文旨在批判性地评价这些共识。

目前隐私立法提案中的诸多方面本质上都趋于保守,作用不大。借用行为心理学家亚伯拉罕·马斯洛(Abraham Maslow)的话来说,目前的提案都在不同程度上拿着办法找问题,而不是根据问题找办法(Maslow,1966)。也有人把马斯洛的观点概括为:"如果你只有一把锤子,什么东西看起来都像钉子。"马斯洛对如何构建解决新问题的方法的讨论,对隐私法的设计具有重要意义。生搬硬套上一个时代的法律规则,无法解决当今基于监控(surveillance)的商业模式所造成的新问题。但制定一部好的隐私法仍大有希望,关键要认识到治理方式也能创新。

本文第二节讨论了一些围绕个人信息隐私权的定义及相关主张而形成的共识。目前隐私法的立法进路深受既有私法思维的影响,主张通过确立个人数据权进行自下而上的治理。这种方式难以对网络化进程中的大规模数据处理进行有效治理。第三节讨论了公共治理(public governance)问题。许多提案确定了

---

* 本文原标题为"How (Not) to Write A Privacy Law",英文原文见 https://knightcolumbia.org/content/how-not-to-write-a-privacy-law,经授权翻译发表。

** 朱莉·科恩(Julie Cohen),美国乔治城大学法学院。

*** 李汶锴,比利时布鲁塞尔自由大学法学院;张月明,比利时根特大学法学院。

公共治理的监管架构,但引用的公法机制已经过时,无法应对当今由数据驱动的网络化进程。有效的隐私治理需要一个能处理好设计、数据流动和规模化等问题的监管模式。我提出了这种模式的一些基本要素,以及一些具体策略,供立法者和监管者参考。第四节评估了立法提案中所提出的落实新的权利和义务的执法机制。现有提案一般从这两种模式中择其一:创设个人诉讼权,或由执法机关启动执法程序。但我认为这两种模式都不能保证有效。并且,关于私人诉讼与公权力执法的争论分散了人们对其他更有效的公共执法机制的注意力。关于如何设计有效的公共执法机制,我认为有三条替代路径可供考虑。

二、以权利为基础的治理:大教堂阴影下的立法[①]

目前,已经颁布的个人信息隐私法和最近几部立法提案普遍受到了同一种治理范式的影响,即依赖个人对权利的主张来实现社会目标,这种范式根植于美国的立法传统。提交国会的隐私立法提案中虽然没有一部直接认可个人对其数据享有财产权,但几乎所有的提案实际上都采用了财产权进路作为基本架构。在这样的架构之下,个人控制权(individual control rights)成为管理个人数据收集和处理的主要机制,而集体层面的持续管理很少被提及。但个人控制权具有分散化、事后性的特点,无法有效规制大规模、网络化的数据处理,也无法改变事先设定的算法和交互界面。

第 116 届国会提出的大多提案都以赋予消费者对数据的个人控制权为出发点。消费者也可以在事实上放弃所谓的“控制权”,同意数据处理者收集和处理他们的数据。一些提案要求以“事前允诺”(opt-in)[②]机制获取数据收集和处理的主体明确同意的信息,例如众议员安娜·埃舒(Anna Eshoo,民主党,加利福尼亚州)提出的《在线隐私法案》(Online Privacy Act,2019)和参议员爱德华·马基(Edward Markey,民主党,马萨诸塞州)提出的《隐私权利法案》(Privacy Bill of Rights Act,2019)。与此相似,参议员玛丽亚·坎特维尔(Maria Cantwell,民主

① 出自美国法学家圭多·卡拉布雷西(Guido Calabresi)和道格拉斯·梅拉默德(Douglas Melamed)的著名论文《财产原则、责任原则与不可让渡性——大教堂的一个视角》(Property Rules,Liability Rules,and Inalienability:One View of the Cathedral),论文阐述了财产权保护的基本原则和范式。——译注

② “事前允诺”(opt-in),又称“事前明示同意”,即在收集和处理个人数据之前,应当在事前得到数据主体的明确同意,否则视为违法。——译注

党,华盛顿州)提出的《消费者在线隐私权利法案》(Consumer Online Privacy Rights Act,2021)要求,信息处理者对消费者负有责任,并允许消费者在认为这些责任没有被落实时提起诉讼。其他法案则要求消费者以"事后退出"(opt-out)[①]的模式同意数据收集和处理,如参议员罗恩·怀登(Ron Wyden,民主党,俄勒冈州)起草的《管好自己的生意法案》(Mind Your Own Business Act,2019),参议员玛莎·布莱克本(Marsha Blackburn,共和党,田纳西州)起草的《平等负责地平衡网络用户权利法案》(Balancing the Rights of Web Surfers Equally and Responsibly Act,2019)。[②]

目前,各部法案对于事前允诺抑或事后退出机制的选择有所不同,但形成的共识对同意机制的设计至关重要。其中一些法案详细地设计了同意的机制,另一些法案则交由执行机构制定细则。举例来说,两部在州立法层面较为严格的法案《伊利诺伊州生物信息隐私法案》(Illinois Biometric Information Privacy Act,BIPA,2008)和《加利福尼亚州消费者保护法案》(California Consumer Protection Act,CCPA,2018)均采用了"个人控制权+同意机制"的制度设计,其中 BIPA 对于生物信息采用了事前允诺机制,而 CCPA 则建立了对于一般个人数据的事后退出机制。

令人费解的是,这些法案对基于同意的隐私治理路径一直保持乐观的态度。众所周知,这种进路的弊端很难避免。很多法案试图建立新的程序性规定,还有些法案则授权执法部门建立一套记录消费者选择的系统,例如怀登起草的《管好自己的生意法案》、参议员乔希·霍利(Josh Hawley,共和党,密苏里州)起草的《"请勿追踪"法案》(Do Not Track Act,2019)。但一些隐私学者则一针见血地指出,这些规定不太可能有效。简而言之,用户为了理解同意的意义而需要了解的情况过于复杂,而同意的条件又极易被操纵(Acquisti,Taylor & Wagman,2016; Draper & Turow,2019; Hartzog,2018)。大多数关于用户控制权的表述都没有考

① "事后退出"(opt-out),即在数据收集和处理过程中,默认用户已经同意了其数据处理活动,用户如不同意,可以通过退出机制实现拒绝权。——译注

② 其中《管好自己的生意法案》要求构建一个不追踪用户的数据共享的事后退出同意机制;《平等负责地平衡网络用户权利法案》提议针对敏感用户信息通过事前允诺方式获取同意,针对非敏感用户信息通过事后退出机制获取同意。

虑到用户行为信息,使科技公司使用合成数据(synthetic data)[①]成为可能,而合成数据也是广告行业商业模式的核心(Edwards & Veale,2017; Veale,Binns & van Kleek,2018; Edwards & Veale,2018; McNamee,2016)。另外,在使用大数据对机器学习模型进行训练时,现有观点也没有考虑到用户针对其中一部分数据撤回同意的后果(Edwards & Veale,2017; Edwards & Veale,2018)。

此处我希望指出的问题是同意机制缺少总体上的有效性:以个人控制权为基础的监管是一种更为个人层面的治理,而且具有事后性。面对模块化的界面,个人用户在被事先定义好的选项中选择时,无法改变那些隐藏的商业安排和技术设计[②],而信息处理者正是凭借这些商业安排和技术设计使数据在多方之间传输。同样,个人用户也无法阻止信息处理者使用对其数据进行进一步分析所获得的推测数据(inference)。即便个人用户通过事后退出机制拒绝了数据的收集,信息处理者也能够继续使用这些推测数据。

长期以来,人们将财产权作为集体秩序维持机制的思维定式,造成了对这种自下而上、依赖个人权利的治理模式能够发挥作用的错误假设。传统财产权理论认为,将获取和使用资源的决定权授予能够最明智和有效地行使它的人,可以形成内部激励,从而使治理成本最小化(Merrill & Smith,2000; Smith,2002)。当代学者也的确指出,财产权理论无法解决某些类型的共同损害(collective harms)(Smith,2009)。即便如此,这些学者依然认为,由于集体管理(collective governance)的成本很高,财产权进路在大多数情况下都应作为默认选项。如果资源的获取和使用权需要转让或合并,财产所有者可以通过谈判达成合意。这种情况下,外部监管就成了个人控制权的例外。这是外部监管的特点,并不是缺陷(Smith,2009)。以此类推,人们可能会认为,利用个人控制权(及其理论上对自我监管的刺激作用)是引导数据收集和处理活动并实现其他监管目标最为有效的方式。并且,公平而言,这种在个人层面的、自下而上的治理方式,在一对一谈判中具有一定的意义,例如不动产交易条件的谈判,或是医疗场景下病患的同意。但出人意料的是,在涉及集体利益的情况下,例如有效的土地规划和使用或医学研究伦理,这种对个人控制权的依赖则屡屡失败(Benjamin,2019; Coleman,

① 合成数据(synthetic data)是人工生成的数据,保留或模仿了真实数据集的属性,同时掩盖或删除了与个人有关的信息。——译注

② 最典型的例子是暗黑模式(dark patterns),指具有误导或欺骗性质的用户界面设计。——译注

2004；Fennell，2012；Kim，2019；Mitchell，2001；Noble，2018；Randall，1996）。因此，只要涉及网络化、大规模的数据处理，个人控制权就失去了意义。

另外值得一提的是，这种财产权思维不仅体现在各隐私法提案所要确立的权利上，还表现在一些数据保护的例外规定中，这些规定严重减损了对于数据处理者的问责效果。在以欧盟成员国为代表的一些法律框架下，出于执法或国家安全目的的数据处理不能免除其数据保护义务，尽管数据处理的形式和内容较为特殊。而在美国，执法和维护国家安全的活动具有特殊性，与之相关的数据处理活动往往完全不受数据保护义务的约束。以第四修正案的相关判例为例，法院常常将数据控制权划分为个人控制权和政府控制权两个独立的部分。政府对数据的获取可能要遵守更高的程序性要求，但一旦数据被合法获取，就被纳入政府的控制范围（Carpenter v. United States，2018；Riley v. California，2014；United States v. Warshak，2010）。其他关于信息收集的法规也往往遵循相同的模式，几乎不会提及政府合法获取数据之后的处理要求（Stored Communications Act，1986；Wiretap Act，1986）。只有美国国家安全相关立法稍显例外，至少纳入了数据保护法学界熟悉的“数据最小化”等概念［50 U. S. C. § 1801（h），2016；50 U. S. C. § 1806（a），2016；Renan，2016］。然而，出于国家安全目的的数据处理活动的不透明性也大大限制了开展集体治理的可能，并且缺少类似于欧洲人权法院赋予公民个人的事后救济渠道。[①] 在第 116 届国会上提出的隐私法案中，没有任何一项涉及政府处理数据的问责制度，因此无法弥补欧盟法院在宣布《欧盟—美国隐私盾协议》[②]无效的判决中所指出的美国数据立法的问题（Schrems and Facebook Ireland v. Data Protection Commissioner，2020）。

一些观点认为，以用户为中心的数据合作社（data cooperatives）[③]将隐私交互设计和隐私条款的选择权交还给个人，或许能使大规模的同意获取在大数据

① 欧盟法院在 Schrems Ⅱ 案［Case C－311/18，Schrems and Facebook Ireland v. Data Protection Commissioner（2020）］中认为，虽然包括欧盟数据主体在内的个人在出于国家安全目的而受到非法电子监控时，美国法提供了许多补救措施，但美国情报当局可能使用的一些法律依据（如第 12333 号行政命令）存在例外。此前，欧盟法院在 Schrems 案［Case C－362/14，Schrems v. Data Protection Commissioner（2015）］中已做出判决，认为美国政府对个人信息的使用“超出了保护国家安全的绝对必要和相称的范围”，而且“数据主体不具有行政或司法补救手段”。

② 该协议旨在允许出于商业用途将欧盟公民的数据传输到美国。

③ 数据合作社（data cooperatives），指出于有利于团体或社区成员的某种目的，个人自愿合作汇集其个人数据的组织。——译注

和网络化时代成为可能(Bietti,2019; Posner & Weyl,2018)。然而,现实中并不存在这样的先例,这种假想的前景也不乐观。有两个原因:第一,如果这一观点基于经济学理论中治理公共资源的集体机制,那么(将经济学原理运用到数据治理中时)人们往往会忽视这种机制运作的前提。集体治理在小规模、同质化的社群中,且资源的边界相对清晰时是更为有效的;社群规模扩大、异质性增加,以及资源更难清晰界定时,这种治理方式的效果就大打折扣(Frischmann, Madison & Strandburg,2014; Ostrom,1990)。第二,社群内成员的权力差异也限制了集体治理规模的扩大。因此,举例来说,在互联网开发者主要由业余爱好者和科研人员组成的 20 多年里,开源许可的规模还相对较大;而大型营利性科技公司的出现加剧了利益冲突,开源许可的规模就大不如前了。“知识共享许可协议”(the Creative Commons Licensing)体系的规模从未覆盖大型的、以营利为目的的利益集团(Cohen,2018)。

要明确的是,基于个人同意的规定确实会激励业界对个人信息流动治理方式的创新;只是这种由企业发起的创新不太可能增强个人控制权,或提供更好的隐私保护。相反,同意作为个人数据的主要治理机制,已经衍生出一种类似于集体组织在管理知识产权时所使用的“增加责任条款”(contracting into liability rules)的模式(Merges,1996),这种模式十分适合用于对大量低价交易的批量化许可。这种模式因而催生了一种适合规模化运作的数据治理方式,但为用户提供标准化选项这一做法,一定会在细节层面阻碍用户给出的同意真实有效。例如,由于欧洲数据保护法要求在许多类型的数据处理中获得个人的明确同意,一些无法承担合规成本的小型企业已经开始联合起来,提供“自动同意管理面板”(automated consent management panels),用户可以通过这一工具向所有加入联合组织的企业表达是否同意(Nouwens,Liccardi & Veale et al. ,2020)。这种方式使同意机制沦为一块遮羞布,用来展示对这种仅在个人层面存在的数据保护制度象征性的合规,而用户仍然无法要求改变信息处理的基本条款或网络服务的设计架构。我们可以预想到,如果美国采用类似于欧洲的同意获取规定,这种自动同意管理面板会在业界被迅速采用。

简而言之,寄希望于分散化治理或集体治理的想法,都反映了对私人秩序(private ordering)落后且根深蒂固的依赖,缺少事实上的依据。无论主张个人控制权、自下而上进行治理的观点,还是集体治理的观点,都忽视了目前大规模数

据处理在结构上和时间上带来的挑战。有效治理需要公权力的监督,也需要对如何构建和实施这种监督进行新的思考,这是下文将要探讨的内容。

三、监管范围与监管路径:“马斯洛之锤”一次又一次砸下

假设隐私法应当优先考虑有效的公共治理,而不是分散化、事后性的个人控制权,那么隐私治理又当如何运作?第116届国会上的提案大多落入“马斯洛之锤”的陷阱:仅仅依赖既有的公共治理工具,无法真正实现对隐私问题进行有效治理。

建立公共治理体系的第一步是选择行使监督权的主体。多数提案提出将监督权赋予联邦贸易委员会(the Federal Trade Commission,FTC),或出于保护选民隐私的目的,赋予联邦选举委员会(the Federal Election Commission,FEC)。监管机构的选择十分重要,因为各机构的管辖范围往往受到某些限制,但设定这些限制之初并没有考虑到信息经济是高度网络化的。举例来说,信息企业作为公共运营商(common carrier)时,对其具有管辖权的不是联邦贸易委员会,而是联邦通信委员会(the Federal Communications Commission,FCC),后者从而在这一事项上具有了限制前者的权力。因而,只有少数提案提出将公共运营商的管辖权限一并移交联邦贸易委员会。另外,受政治性原因影响,联邦贸易委员会的规则制定权和执法权与其他独立机关相比受到诸多限制,且掌握的资源有限。这反映了人们不愿赋予消费者保护机构过多干预市场活动权力的倾向。无论提出这些提议的议员是否承认了这一点,将联邦贸易委员会设为隐私执法机构且扩大其权限范围的做法,事实上表明他们已经认同了这一选择(Hoofnagle,2016)。而联邦选举委员会也仅有权管辖有关竞选的宣传活动(electioneering communications),且资源也相当有限。即使通过修改相关定义,使数字广告等同于电视广播广告,联邦选举委员会也无权管辖一些最强大且最有害的、由网络数据驱动的不实信息和虚假信息(Cohen,2020; Hasen,2022)。[①] 那些承诺通过提高数字选举活动的透明度来打击选举操纵行为的提案,似乎并不了解这一点。

① 不实信息(misinformation),指错误的但并非以造成伤害为目的的信息;虚假信息(disinformation),指为了伤害某个人或组织而刻意虚构的信息。——译注

然而,即使一些主张建立新的隐私监管机构的提案,也无法避免“马斯洛之锤”的诱惑。接下来我们考察两种越来越受推崇的监管路径。

第一种路径借用并重构信托法和公司法中基于信任的概念。这一路径主要有两个分支:一种是明确信托义务中包含哪些面向,例如保密、注意和忠诚(confidentiality,care and loyalty)义务;另一种则主张直接采用更为笼统的信用(trustworthiness)义务(Balkin,2015; Balkin,2020; Richards & Hartzog,2021)。两种主张在论证过程中都采用了类比其他信托协议的进路。由于生成个人数据的做法与定向广告(targeted advertising)相关,用户会与很多不同的平台服务提供者签订长期协议,这种具有历时性的、跨场景的协议关系(理论上)可能成为引入更高水平信托义务的依据。然而,批评的声音也指出,信托义务的概念其实很难在公司场景下全面适用,因为管理者的自身利益和对股东的短期义务会导致公司不愿承担公共责任(Khan & Pozen,2019)。当然,也可以通过明确规定谨慎和忠诚义务来限制公司这种利己主义和追求短期利益的行为(Haupt,2020; Richards & Hartzog,2021; Tuch,2020)。

但是,如何在网络化数字经济的背景下建立信任,甚至比在企业语境下引入信托机制的讨论更加复杂。如今,(用户与平台的)关系被重新定义为大众—市场产品(mass-market products),并且这种关系是通过为大型网络化互连互通而设计的标准化用户界面来实现的。在此背景下,仅承认服务关系的意义并不大(Becher & Dadush,2021)。在关系即产品的时代,关于产品安全的法律和监管已经变得更严格。我们当然可以用“信任”一词来描述产品设计领域的义务和标准体系。比如,当我坐在办公室里的椅子上时,我有理由确信椅子不会塌。然而,我怀疑大多数现代法律人士都会认为这种表述过于笼统、没有意义。毕竟当事故发生时,能够具体地谈论材料耐久度和制造规格等问题,并且能够援引相应的侵权和监管法律条文,要比空泛地谈论我与椅子制造商之间关系的性质有用得多。

关于设计与监管关系的讨论,已经超越了消费品制造业,延伸到一系列复杂的、信息密集型的产品和服务。事实上,许多复杂的产品和服务都已经受到了全面的监管。我们可以期待,制药公司应该对那些服用他们生产的药物的人承担谨慎、注意、忠诚和科学诚信(scientific integrity)的责任,保险公司应该对他们的投保人承担谨慎、注意、忠诚和精算诚信(actuarial integrity)的责任,而银行应该

对他们的储户承担谨慎、注意、忠诚和保证偿付能力(solvency)的责任。但是,对这三类行业的公共治理都已经很健全了,以至于大多数人都会认为这些责任的设置对治理那些“关系即产品”的行业并无助益。

分配监管权力的第二种路径是利用反垄断法中的关于市场支配地位的概念。例如,一些提案针对具有一定规模的信息企业设置了特别的信息披露和报告义务(Consumer Data Privacy and Security Act,2020; Mind your Own Business Act,2019)。[①] 从概念上来说,这些提案与强制要求科技巨头进行拆分并重组的措施相对应,但也存在部分的相对限缩(企业分拆和一些其他反垄断干预措施也可能在第117届国会中被提上议程[②])。但反垄断的方法并不能很好地解决监控滥用的问题。长期以来,反垄断法在面对如何分配具有竞争性授权的无形知识产权、网络信息系统中的市场支配等问题时,也面对着如何控制由技术和法律协议构建的网络化的数据流的难题(Guggenberger,2020; Weiser,2002)。为了使针对市场支配者的措施能够有效地规制基于监控的商业模式,不仅需要改变公司的所有权和治理结构,还需要改变通过许可协议授权传输数据的模式。尤其是,占支配地位的平台为软件开发者提供的工具包中往往包含开发者并不了解的数据收集和传输协议(Sankin & Mattu,2020)。因此,以限制市场支配地位为目标的隐私法必须明确指出,数据流如何通过由多个行动者构成的关系网络被设计、嵌入、分层、隐藏和传播。此外,旨在打破占市场支配地位的企业通过许可协议对数据流进行垄断的措施,如果不与其他隐私保护措施相结合,隐私保护状况只会更加恶化。

更广泛地说,网络信息经济的功能失调反映了数据流动网络化、规模化的问题,这与现有的市场支配问题是十分不同的。信息经济的监管面临着保罗·欧姆(Paul Ohm)所称的“数量级问题”(order of magnitude problem)——网络化的信息流动表现出规模化的影响(Ohm,2018)。市场支配在这一过程中的影响十分重要,占支配地位的法律主体的自利行为会加剧“数量级问题”的危害。但即便市场中不存在占支配地位的主体,网络化现象也能产生规模化的效应。这是

① 例如,《消费者数据隐私与安全法案》提出加强对大型企业的管理要求,并减轻小型企业对于满足消费者行使访问权的义务;《管好自己的生意法案》提出加强对大型企业报告义务和向用户负责的要求。

② 一个提出类似主张的例子:Staff of Subcomm. on Antitrust, Com. and Admin. L. Comm. on Judiciary, 116th Cong., Investigation of Competition in Digital Markets (2020).

因为在网络化信息生态中处于边缘地位的小型主体倾向于利用占支配地位的大平台的服务和能够连接全人类的信息网络。不管是新兴的媒体公司,还是虚假信息的生产者,以及宣扬仇视和种族至上的极端主义者,都正在采用收集、处理和利用个人数据的策略。他们不断学习如何在多个平台和应用中优化内容,使其更适合网络化、社会化的传播(Nadler, Crain & Donovan, 2018; Petre, 2015)。为了确保有效性,隐私治理制度也需要考虑数量级问题,使监督和执法权力相应地增强和扩展。

一些欧洲学者认为,美国隐私法提案最大的问题是没有采用第三种路径——设置一套"欧洲式"的数据保护义务体系。这种体系覆盖了所有实体,不论其市场规模或市场地位,并且比信托原则更直接和全面。尤其是数据最小化和目的限制原则,被认为将有效规制以信息为中心的商业模式运作。① 美国的政策制定者很大程度上默认了科技企业的主张,认为隐私法应当为已收集的数据的再利用留出广泛的可能性,以此推动科技创新。因此,不出所料,最近提交给国会的大多数提案都没有认真考虑目的限制原则(Cohen, 2019)。

第三种路径一个更根本的问题是,如果仅依赖于企业的审慎义务,而不对数据的收集和使用行为进行细致的结构化限制,它将招致严厉的批评。制定数据保护法最初的目的是建立一套允许信息收集和传输,并为数据主体提供适当保障的规则体系(Palka, 2020)。欧盟《通用数据保护条例》(General Data Protection Regulation, GDPR, 2016)规定了数据保护设计和默认数据保护(data protection by design and by default)的实质性义务,但并没有具体说明这种义务所要求的各种设计实践方法。正是实质性标准的缺失导致了执法行动中出现问题,数据保护监管机构经常依靠所谓"违反信息披露义务"的理由进行执法活动,反而回归了用户控制权这一阻力最小的途径,回到了分散化治理的道路(Jones & Kaminski, 2020; Palka, 2020)。

简而言之,尽管构建信任的路径和反垄断的路径的缺点都加剧了基于监控的商业模式的功能失调,但要充分应对这些问题,就必须克服数据保护的被动性,建立可以应对设计,网络化、规模化数据流动的新问题的治理模式,并以收集、处理和交换个人信息的具体要求为框架。

① 参见欧盟《通用数据保护条例》第五条(1)(b)-(c)。

然而,监管机构如何设计和执行这样的监管思路呢?在这里,“马斯洛之锤”的陷阱再次出现。立法者在授予监管权力时仍倾向于假设监管者能够使用已有的工具来追求他们的立法目标。这些工具主要是已经有百年历史的经济监管手段,大量证据已经表明它们是无效的。

在立法过程中,关于监管工具的问题往往最后才被考虑到。立法者似乎把监管工具局限在一个相对确定的范围之内。如果有人想使一个新问题获得监管者的注意,或者相反,想要不引人注意地进行改革,那么他就会将制定细则和执法的权力交由下位法的制定者,等待通过这种方法收获想要的结果。许多提案都遵循了这个老办法,即使它早已无效。即便是一些非正式的规制手段,也被证明完全不适合约束网络化、高度信息化的活动,因为这些活动及其相关的知识领域发展得太快(Brummer,2015; Hu,2014; Ohm,2009; Weiser,2009)。执法工作本身很大程度上已演变为标准化的征求同意的操作,创造了法律内生性的过程,这同时内化和弱化了实质性的要求(Cohen,2019; Edelman,2016; Waldman,2019)。其他领域确实提供了更多样化的监督手段,特别是当代金融监管。这些监管手段本身在过去 25 年间经历了快速变化,其中有很多策略可以被隐私监管机构借用和改造。但它们往往需要生长于预先存在的监管环境中,这阻碍了(隐私治理领域)对这些工具进行有益尝试。

提高监管机关隐私治理的有效性,需要从三个方面打破惯例,才能实现监管上的创新。

首先,也是最基本的,有效的隐私治理需要一套现代化的监督制度,以及有能力发展和施行这些制度的人员。隐私监管机构的手段和工具,可以在概念上,从消费者金融监管中借鉴一些设计标准;从银行监管中借用审计、基准和压力测试等操作要求;从一些监管领域中借鉴监测要求;等等(Baradaran,2014; van Loo,2016; van Loo,2019a; van Loo,2019b;Willis,2015)。在专家帮助下开发的其他类型的工具也同样重要,这些工具可以用来应对如暗黑模式(dark patterns)、算法偏见(algorithmic bias)以及网络威胁建模(network threat modeling)等问题(Hartzog,2018; Engstrom,Ho & Sharkey et al.,2020)。

其次,采用新的监管手段需要打破根深蒂固的“私有部门代位监管”(privatized oversight)的模式,这种模式并非监管中真正的“公私合作”。在越来越多的经济部门中,监管机关已变得更加依赖第三方审计师、技术供应商和其他

专业中介机构来评估监管对象是否合规(Bamberger,2006; Bamberger,2009; Waldman,2019)。正如马尔戈特·卡明斯基(Margot Kaminski)指出的,新出现的隐私“二元治理”(binary governance)模式反映了这一趋势;阿里·沃尔德曼(Ari Waldman)也认为,虽然监管的覆盖范围日益扩张,但合规却有了越来越多的“表演性质”(Kaminski,2018; Waldman,2021)。尽管第三方中介机构在扩大治理机制覆盖面上发挥着重要作用,但在网络信息时代,监管机关对中介机构的问责机制不可或缺。换句话说,将权力下放给同时是自利行为者的实体,与授权这些组织代表公权力进行监管活动是有区别的。

最后,在隐私治理制度中,网络信息生态系统的参与者和监督其运作的监管者都应承担信息公开披露义务(public transparency obligation)。为了有效实施这一点,法律及实施细则需要预见到财产权思路在这一方面仍有持续的影响力,因此必须细化信息披露义务。《联邦信息自由法案》(Freedom of Information Act,1967)是目前规定信息披露义务的主要法律,该法案第一部分在本质上也采用了财产权逻辑,而过多豁免条款的存在更加印证了这一思路。一些豁免条款使国家安全和执法行动免于审查,强化了把信息转移到这些领域就意味着放弃了个人信息控制权这一说法。另一些豁免条款则保护所谓的“商业秘密”和范围更广的“保密信息”(confidential information),强化了事实上的排他性权利,甚至政府部门也无法获取此类信息(Graves & Katyal,2020)。新兴的个人数据处理“二元治理”的惯例往往重复这些错误,没有保留面向大众的信息披露要求(Kaminski,2018)。要尊重公众的知情权,就不能盲目满足网络信息时代普遍存在的保密要求。

在第 116 届国会上的隐私法提案中,只有两项与上文所述的这种隐私治理方式相近,分别是众议员安娜·埃舒(Anna Eshoo,民主党,加利福尼亚州)提出的《在线隐私法案》(Online Privacy Act,2019)和参议员柯尔斯顿·吉利布兰德(Kirsten Gillibrand,民主党,纽约州)提出的《数据保护法案》(Data Protection Act,2020),但这两项提案也存在着致命缺陷。埃舒的提案将创建一个独立的数字隐私监管机关,并赋予其强大的执法权力,但该机关的规则制定权将主要针对一系列急剧扩大的个人控制权的侵权行为;吉利布兰德提出建立独立的数据保护机关,将监督一系列“高风险的数据处理行为”,包括用户画像(profiling)和生物识别数据及其他敏感数据的处理,但对该机构规则制定权和执法权的限制条

件与目前对联邦贸易委员会的限制较为类似。此外,在第116届国会期间,参议员谢罗德·布朗(Sherrod Brown,民主党,俄亥俄州)提出的《数据问责和透明度法案》(Data Accountability and Transparency Act,2020)也被保留在考虑范围之内。该提案对个人数据的公共治理进行了更全面的重构,禁止某些类型的个人数据处理活动及各种形式的基于数据的歧视行为。该法案提出设立一个独立的数据保护机关,赋予其执行这些禁令的权力,以及监督自动决策系统测试的职责。同样,布朗的提案也保留了一套控制权,并仿照《联邦贸易委员会法案》限制联邦执法权。然而,其中更具创新性的条款可能会成为网络信息时代隐私治理制度的核心,值得被继续认真考虑。

四、权利救济抑或行政执法:在糟糕和更糟糕之间的选择

制定隐私法的第三个重要共识与法律的执行机制有关。尽管在是否允许个人提起侵权诉讼上存在较大分歧,但在执法机制有哪些选择这一问题上,各方的意见是一致的。一般来说,针对隐私侵权有两种主要的执法方式:一是由个人提起诉讼,二是由执法机关启动执法程序(Kerry,Morris & Chin et al.,2020)。无论哪一种,都以诉讼为主要手段,且具有事后性,并不能有效制约科技巨头过度处理个人数据的行为。如果仅在二者之间选择,会错失其他更有效的、对网络化信息流动带来的风险更有针对性的方案。

需要明确的是,由个人提起的诉讼和由执法机关启动的执法程序,都要具有表达性和规范性功能。执法机关对公然的违法行为的打击、对体现法律所表达的价值观具有重要作用。至少在理论上,确保这种执法程序充分的覆盖面,可以展现政府制约相对强大的营利性实体、依法保护公民利益的承诺(McAdams,2015;Sunstein,1996)。赋予公民通过诉讼维护自身合法权利的能力,至少要求相对方对其行为做出说明,也是这种承诺的体现。并且,取决于不同的结构,有的执法程序还具有维护公民人格利益的重要功能(Bayefsky,2020)。

即便如此,关于以诉讼为中心的执行机制的相对和绝对效果的讨论,反映了对诉讼的优势的反思。近几十年来,对起诉及集体诉讼资格和范围的批判,极大地限制了通过诉讼主张个人利益损害的可行性(Solove & Citron,2017;Schipani

& Dworkin,2012; Hensler,2007)。在很大程度上,个人无法通过诉讼的方式维护自己的新型信息隐私权。同时,公权力执法机关的资金长期不足。近几十年来,这些机关在很大程度上默许了协议裁决(consent decree)这一惯例,将大部分监督权下放给私人审计师和企业内部合规人员(Cohen,2019; Waldman,2019)。

回到第二节的讨论,出乎意料的是,人们一致相信诉讼——无论是个人发起的,还是公权力机关发起的——是一种有效的救济手段。这从两个互补的角度反映了财产权思维的影响。

第一,诉讼在确定和评估损害方面仅针对个案,不能有效解决网络化所导致的大规模集体损害。这种不匹配的问题在个人诉讼中最为明显。个人诉讼依据个人所遭受的损害确定赔偿额,即使是集体诉讼或新型的多地区联合诉讼机制也没有更为有效(Cohen,2016)。然而,行政执法机关的执法行动也没有更为有效。由于资源极其有限,执法人员会仔细考虑并选择可能产生最大影响的执法目标。这种选择性的执法方式往往只是确认了某种主流违法模式的存在,不能从根本上解决问题。但是,如果执法机关普遍将主流以外的小型行为主体列为执法目标,那么这些小企业的力量也不足以推动它们上游的网络化进程、协议和用户界面的革新。

第二,诉讼往往体现出与财产权思维相同的、自下而上的治理方式,因此无法回答“应当如何纠正违法行为”这一问题。上文提及,财产权思维通过外部成本的强制内部化激励财产所有者遵守规则,而由其自行决定如何实现内部治理。然而,现实是,除非有更具体的规定,否则这种方式并不能持续性地改变违法行为。相反,特别是当违法行为可以带来巨额利润,又相对较难被发现时,违法者会将偶尔的处罚视为经营成本。总的来看,联邦贸易委员会的隐私执法结果,包括在剑桥分析公司(Cambridge Analytica)丑闻[①]曝光后对脸书(Facebook)发出的广为人知的处罚在内,都印证了这个规律。过去 20 年里,科技行业对基于监控的商业模式的依赖实际上只增不减(Cohen,2019; Zuboff,2019; Zuboff,2021)。

下文简要提出了三种可行的执法机制,或许能产生更深远且持续的执法效

① 英国咨询机构剑桥分析公司(Cambridge Analytica)在未经脸书用户同意的情况下获取 8700 万脸书用户的个人数据,用于投放政治广告,包括在 2016 年美国总统大选中为美国前总统特朗普提供帮助。2020 年 4 月,美国联邦法院批准了脸书与美国联邦贸易委员会就剑桥分析丑闻的 50 亿美元和解协议。这起丑闻引发了公众对社交媒体泄露个人隐私的担忧。——译注

果。这些选项不是穷尽的,本文并不试图列举所有的可能性,而是希望打破根深蒂固的思维定式,鼓励针对网络化进程、协议和用户界面设计的执法策略进行创新,并随着相关行为规模的增长相应地扩大这一执法实验。以下每项建议都至少出现在一个待议的隐私法提案中,但并未受到华盛顿立法者们的重视。并非巧合的是,这些建议与第三节所述更主动的隐私治理方式相配合,很可能是推动执法变革唯一现实的方案。

加大执法力度的一个基本策略是,利用"守门人"(gatekeeper)[①]的力量来落实政府监管中有关设计、操作和监测的规范。对于作为网络服务提供商的信息企业来说,这将几乎颠覆它们对于在多大程度上需要对第三方行为负责的普遍判断。然而,正如范卢(Rory van Loo)所言,从监管的角度来看,这种平台代理执法并不是常规的手段;但对于业界来说,"守门人"作为执法代理人帮助落实企业行为准则,是至关重要的,也是可接受的(van Loo,2020; Willis,2017)。同样,要求大型网络平台代执法机关管理其创建的信息生态系统中较小的参与者是完全合理的,毕竟它们在这一生态中获取了巨额利润。此外,有人认为这种"代理执法"制度必然会沦为审查制度(censorship),但在其他领域存在的类似制度可以证明,这种精心编造的观点是站不住脚的。这种机制的有效性已有先例,如网络平台可以为软件开发工具包中数据收集和交换功能制定标准,也可以为个性化推荐设定外部限制,以优化网络化、社会化的内容传播。

为了确保执法的有效性,扩大执法的同时也应当加大对违法者的处罚力度。众所周知这十分困难,而且已经远远超出了隐私立法的范畴。然而,事实上,大型科技公司在美国和其他的地区一再消极地应对处罚决定,表明它们可能对一般数额的罚款已经免疫。剑桥分析公司丑闻曝光后对脸书的处罚就是一个例子——50 亿美元的罚款,虽然已经是迄今为止联邦贸易委员会所发出的最大罚单,但只相当于这个科技巨头一个月的收入(Patel,2019)。正如保罗·欧姆所指出的,产生"数量级效应"的违规行为需要受到相应力度的制裁(Ohm,2018)。

一个经常被忽视的执法手段是没收违法所得,其数额之大是普通罚款所无法比拟的。美国最高法院最近确认,即使没有明确授权,联邦法院也可以运用其

① 隐私和数据保护法语境下,"守门人"(gatekeeper)一般指在规模上达到某些预设的基准(如用户数量、业务类型、营业额等),为其他企业的产品和服务提供平台,因此能对互联网生态产生巨大影响的大型网络服务提供者,例如谷歌和亚马逊。——译注

固有的衡平法权力下令没收财产(Liu v. SEC,2020)。目前几个执法机关,包括联邦贸易委员会和证券交易委员会,在某些类型的案件中都有判处没收违法所得的权力(AMG Capital Mgmt. v. FTC,2020)。在第 116 届国会上提出的隐私法提案中,只有两个提案规定了这种处罚措施(Data Protection Act,2020; Online Privacy Act,2019)。[①] 然而,目前对没收财产的概念化往往包含了本文第二节所述的分散化的治理方式。无论是司法机关行使固有的没收财产的权力,还是现有的执法机关行使这一权力,都往往需要先确立一个可追溯的经济损失计算标准,而可追溯性在许多主张信息隐私损害的案件中都无法实现。为了在隐私保护方面发挥最大作用,没收违法所得应遵循按公开程序制定的有关设计、操作和监测的要求。隐私立法应当明确规定,没收违法所得是对此违法行为的纠正措施,并应授权监管机构确定违法所得金额的标准,以及根据"数量级效应"建立对追偿额进行调整的机制,并向公众证明这些机制的合理性(Ohm,2018; Liebmann,2019)。最后,也很重要的一点是,与其向每个受影响的个人分配几美元的赔偿,不如将追偿的部分资金用于执法机关的监管行动。

另一个未被提及的执法手段,是对阻挠和破坏隐私监管的公司高级管理人员和董事会成员追究个人责任。作为选择之一,隐私立法可以授权公权力机关对故意违反规则、破坏公司集体治理程序完整性的公司主管实施刑事制裁(Mind Your Own Business Act,2019)。然而,现实中,在公司语境下确定犯罪意图可能十分困难。这在很大程度上是因为,破坏真正变革的法律内生性,也会在违法行为发生时起到否定犯罪意图的作用。一个确认个人责任更实际的方法,是借用并改造公司法中"刺破公司面纱"的机制。特别是当侵犯隐私的公司采用双层所有权结构,以保证创始人和风险投资者占优势的投票权时(现在多数家喻户晓的科技巨头都是这种模式)(Molla,2019),对通过滥用监控用户这一手段而赚取的个人财富采取处罚措施更加合理,即使在无法证明公司高层对某一具体的侵权行为知情或具有意图的情况下也是如此。

① Data Protection Act 提出法院或机构可给予的救济包括"撤销或重新订立合同""恢复原状"和"没收或赔偿不当得利"。Online Privacy Act 提出的救济方式包括"撤销或重新订立合同""恢复原状"和"没收不当得利"。

五、结论:立法建议

决策者重视共识,但在经济和技术发生重大变革的时代,共识可能是一把双刃剑。提交国会审议的信息隐私立法提案中所形成的共识就是一个例子:它声称要规划未来的道路,但这种承诺只为因循守旧提供了借口,并进一步加剧了系统性科技监控的滥用。起草一部有效的隐私法案需要采取新的思路。在治理网络化进程的关键时刻,避免捷径的诱惑非常重要,治理机构和手段也应该拥抱创新。本文中,我简要描绘了具备制约大规模网络化进程的公共制度的设计方案,并介绍了立法者可以参考的其他资源。现在正是第 117 届国会开始着重考虑这一问题的时机。

参考文献

Acquisti, A., C. Taylor & L. Wagman 2016, "The Economics of Privacy." *Journal of Economic Literature* 54.

Balkin, J. 2015, "Information Fiduciaries and the First Amendment Lecture." *U. C. Davis Law Review* 49(4).

Balkin, J. 2020, "The Fiduciary Model of Privacy." *Harvard Law Review Forum* 134(1).

Bamberger, K. 2006, "Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State." *Duke Law Journal* 56(2).

Bamberger, K. 2009, "Technologies of Compliance: Risk and Regulation in A Digital Age." *Texas Law Review* 88(4).

Baradaran, M. 2014, "Regulation by Hypothetical." *Vanderbilt Law Review* 67(5).

Bayefsky, R. 2020, "Remedies and Respect: Rethinking the Role of Federal Judicial Relief." *Georgetown Law Journal* 109(6): 1263-1336.

Becher, S. & S. Dadush 2021, "Relationship as Product: Transacting in the Age of Loneliness." *University of Illinois Law Review* 2021(5).

Benjamin, R. 2019, "Race After Technology: Abolitionist Tools for the New Jim Code." https://www.wiley.com/en-us/Race+After+Technology%3A+Abolitionist+Tools+for+the+New+Jim+Code-p-9781509526437.

Bietti, E. 2019, "Locked-In Data Production: User-Dignity and Capture in the Platform Economy." https://ssrn.com/abstract=3469819.

Brummer, C. 2015, "Disruptive Technology and Securities Regulation." *Fordham Law*

Review 84(3).

Cohen, J. 2016, "Information Privacy Litigation as Bellwether for Institutional Change Symposium-Privacy, Data Theft and Corporate Responsibility: Twenty-Second Annual Clifford Symposium on Tort Law and Social Policy." *DePaul Law Review* 66(2).

Cohen, J. 2018, "Property and the Construction of the Information Economy: A Neo-Polanyian Ontology." *Georgetown Law Faculty Publications and Other Works*, https://scholarship.law.georgetown.edu/facpub/2043.

Cohen, J. 2019, *Between Truth and Power: The Legal Constructions of Informational Capitalism*, New York: Oxford University Press.

Cohen, J. 2020, "Tailoring Election Regulation: The Platform Is the Frame." *Georgetown Law Technology Review*, https://georgetownlawtechreview.org/tailoring-election-regulation-the-platform-is-the-frame/GLTR-07-2020.

Coleman, C. 2004, "Rationalizing Risk Assessment in Human Subject Research." *Arizona Law Review* 46(1).

Draper, N. & J. Turow 2019, "The Corporate Cultivation of Digital Resignation." *New Media & Society* 21(8).

Edelman, L. 2016, *Working Law: Courts, Corporations, and Symbolic Civil Rights*, Chicago: University of Chicago Press.

Edwards, L. & M. Veale 2017, "Slave to the Algorithm? Why A 'Right to An Explanation' Is Probably Not the Remedy You Are Looking for." *Duke Law & Technology Review* 16(1).

Edwards, L. & M. Veale 2018, "Enslaving the Algorithm: From A 'Right to An Explanation' to A 'Right to Better Decisions'?" *IEEE Security & Privacy* 16(3).

Engstrom, D., D. Ho & C. Sharkey et al. 2020, "Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies." https://law.stanford.edu/wp-content/uploads/2020/02/ACUS-AI-Report.pdf.

Fennell, L. 2012, "The Problem of Resource Access." *Harvard Law Review* 126(6).

Frischmann, B., M. Madison & K. Strandburg 2014, *Governing Knowledge Commons*, Oxford: Oxford University Press.

Graves, C. & S. Katyal 2020, "From Trade Secrecy to Seclusion." *Georgetown Law Journal* 109(6).

Guggenberger, N. 2020, "Essential Platforms." *Stanford Technology Law Review* 24(2).

Hartzog, W. 2018, *Privacy's Blueprint: The Battle to Control the Design of New Technologies*, Cambridge: Harvard University Press.

Hasen, R. 2022, "Cheap Speech: How Disinformation Poisons Our Politics, and How to Cure It." https://yalebooks.yale.edu/9780300259377/cheap-speech.

Haupt, C. 2020, "Platforms as Trustees: Information Fiduciaries and the Value of Analogy." *Harvard*

Law Review Forum 134(1).

Hensler, D. 2007, "Has the Fat Lady Sung: The Future of Mass Toxic Torts." *Review of Litigation* 26(4).

Hoofnagle, C. 2016, *Federal Trade Commission Privacy Law and Policy*, New York: Cambridge University Press.

Hu, H. 2014, "Disclosure Universes and Modes of Information: Banks, Innovation, and Divergent Regulatory Quests." *Yale Journal on Regulation*31(3).

Jones, M. & M. Kaminski 2020, "An American's Guide to the GDPR." *Denver Law Review* 98(1).

Kaminski, M. 2018, "Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability." *Southern California Law Review*, 92(6).

Kerry, C., J. Morris & C. Chin et al. 2020, "Bridging the Gaps: A Path Forward to Federal Privacy Legislation." https://www. brookings. edu/research/bridging-the-gaps-a-path-forward-to-federal-privacy-legislation.

Khan, L. & D. Pozen 2019, "A Skeptical View of Information Fiduciaries." *Harvard Law Review*, 133(2).

Kim, K. 2019, Consentability: *Consent and Its Limits*, Cambridge: Cambridge University Press.

Liebmann, S. 2019, "Dazed and Confused: Revamping the SEC's Unpredictable Calculation of Civil Penalties in the Technological Era Notes." *Duke Law Journal* 69(2).

Maslow, A. 1966, *The Psychology of Science a Reconnaissance*, New York: Harper & Row.

McAdams, R. 2015, *The Expressive Powers of Law: Theories and Limits*, Harvard: Harvard University Press.

McNamee, J. 2016, "Is 'Privacy' Still Relevant in A World of Bastard Data? European Digital Rights (EDRi)." https://edri. org/our-work/enditorial-is-privacy-still-relevant-in-a-world-of-bastard-data.

Merges, R. 1996, "Contracting into Liability Rules: Intellectual Property Rights and Collective Rights Organizations." *California Law Review* 84(5).

Merrill, T. & H. Smith 2000, "Optimal Standardization in the Law of Property: The Numerus Clausus Principle." *The Yale Law Journal* 110(1).

Mitchell, T. 2001, "From Reconstruction to Deconstruction: Undermining Black Landownership, Political Independence, and Community Through Partition Sales of Tenancies in Common." *Northwestern University Law Review* 95(2).

Molla, R. 2019, "More Tech Companies Are Selling Stock that Keeps Their Founders in Power." https://www. vox. com/2019/4/11/18302102/ipo-voting-multi-dual-stock-lyft-pinterest.

Nadler, A., M. Crain & J. Donovan 2018, "Weaponizing the Digital Influence Machine." *Data & Society*, https://datasociety. net/library/weaponizing-the-digital-influence-machine.

Noble, S. 2018, "Algorithms of Oppression: How Search Engines Reinforce Racism", https://nyupress. org/9781479837243/algorithms-of-oppression.

Nouwens, M. , I. Liccardi & M. Veale et al. 2020, "Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence." Conference on Human Factors in Computing Systems, https://doi. org/10. 1145/3313831. 3376321.

Ohm, P. 2009, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." *UCLA Law Review* 57(6).

Ohm, P. 2018, "Regulating at Scale." *Georgetown Law Technology Review* 546(2).

Ostrom, E. 1990, *Governing the Commons: The Evolution of Institutions for Collective Action*, Cambridge: Cambridge University Press.

Palka, P. 2020, "Data Management Law for the 2020s: The Lost Origins and the New Needs." *Buffalo Law Review* 68(2).

Patel, N. 2019, "Facebook's $5 Billion FTC Fine Is An Embarrassing Joke." https://www.theverge. com/2019/7/12/20692524/facebook-five-billion-ftc-fine-embarrassing-joke.

Petre, C. 2015, "The Traffic Factories: Metrics at Chartbeat, Gawker Media, and The New York Times." https://doi. org/10. 7916/D80293W1.

Posner, E. & E. Weyl 2018, *Radical Markets : Uprooting Capitalism and Democracy for A Just Society*, Princeton: Princeton University Press.

Randall, V. 1996, "Slavery, Segregation and Racism: Trusting the Health Care System Ain't Always Easy! An African American Perspective on Bioethics." *Saint Louis University Public Law Review* 15(2).

Renan, D. 2016, "The FISC's Stealth Administrative Law." in *Global Intelligence Oversight: Governing Security in the Twenty-First Century*, Oxford: Oxford University Press.

Richards, N. & W. Hartzog 2021, "A Duty of Loyalty for Privacy Law." *Washington University Law Review* 99(3).

Sankin, A. & S. Mattu 2020, "The High Privacy Cost of A 'Free' Website—The Markup." https://themarkup. org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites.

Schipani, C. & T. Dworkin 2012, "Class Action Litigation after Dukes: In Search of A Remedy for Gender Discrimination in Employment." *University of Michigan Journal of Law Reform* 46(4).

Smith, H. 2002, "Exclusion Versus Governance: Two Strategies for Delineating Property Rights." *The Journal of Legal Studies* 31(S2).

Smith, H. 2009, "Mind the Gap: The Indirect Relation Between Ends and Means in American Property Law." *Cornell Law Review*(4).

Solove, D. & D. Citron 2017, "Risk and Anxiety: A Theory of Data-Breach Harms." *Texas Law*

Review 96(4).

Sunstein, C. 1996, "On the Expressive Function of Law." *University of Pennsylvania Law Review* 144(5).

Tuch, A. 2020, "A General Defense of Information Fiduciaries." *Washington University Law Review* 98(6).

van Loo, R. 2016, "Rise of the Digital Regulator." *Duke Law Journal* 66(6).

van Loo, R. 2019a, "Regulatory Monitors: Policing Firms in the Compliance Era." *Columbia Law Review* 119(2).

van Loo, R. 2019b, "The Missing Regulatory State: Monitoring Businesses in An Age of Surveillance." *Vanderbilt Law Review* 72(5).

van Loo, R. 2020, "The New Gatekeepers: Private Firms as Public Enforcers." *Virginia Law Review* 106(2).

Veale, M., R. Binns & M. van Kleek, 2018, "Some HCI Priorities for GDPR-Compliant Machine Learning." CHI-GDPR, https://ssrn.com/abstract=3143705.

Waldman, A. 2019, "Privacy Law's False Promise." *Washington University Law Review* 97(3).

Waldman, A. 2021, *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power*, Cambridge: Cambridge University Press.

Weiser, P. 2002, "Law and Information Platforms." *Journal on Telecommunications & High Technology Law* 1.

Weiser, P. 2009, "The Future of Internet Regulation." *U. C. Davis Law Review* 43(2).

Willis, L. 2015, "Performance-Based Consumer Law." *The University of Chicago Law Review* 82(3).

Willis, L. 2017, "Performance-Based Remedies: Ordering Firms to Eradicate Their Own Fraud Consumer Credit in America: Past, Present, and Future." *Law and Contemporary Problems* 80(3).

Zuboff, S. 2019, *The Age of Surveillance Capitalism: The Fight for A Human Future at the New Frontier of Power*, New York: Public Affairs.

Zuboff, S. 2021, "The Coup We Are Not Talking About." *The New York Times*, https://www.nytimes.com/2021/01/29/opinion/sunday/facebook-surveillance-society-technology.html.

立法提案及现行法律

50 U.S.C. § 1801(h) (2016).

50 U.S.C. § 1806(a) (2016).

Balancing the Rights of Web Surfers Equally and Responsibly Act (BROWSER Act), S. 1116, 116th Cong. (2019).

California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.120(a) (2018).

Consumer Data Privacy and Security Act, S. 3456, 116th Cong. (2020).

Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019).

Date Accountability and Transparency Act of 2020 Discussion Draft, 116th Cong., 2020 Session (2020).

Data Protection Act of 2020, S. 3300, 116th Cong. (2020).

Do Not Track Act, S. 1578, 116th Cong. (2019).

Illinois Biometric Information Privacy Act (BIPA), 740 Ill. Comp. Stat. 14/15 (2008).

Mind Your Own Business Act of 2019, S. 2637, 116th Cong. (2019).

Online Privacy Act of 2019, H. R. 4978, 116th Cong. (2019).

Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) (2016).

Stored Communications Act, 18 U. S. C. § 2703 (1986).

The Freedom of Information Act (FOIA), 5 U. S. C. § 552 (1967).

Wiretap Act, 18 U. S. C. § 2518 (1986).

判例

AMG Capital Mgmt. v. FTC, 910 F. 3d 417 (9th Cir. 2018), cert. granted, 141 S. Ct. 194(2020).

Carpenter v. United States, 585 U. S. (2018).

Liu v. Securities and Exchange Commission, 591 U. S. (2020).

Riley v. California, 573 U. S. 373 (2014).

Schrems and Facebook Ireland v. Data Protection Commissioner, CJEU, C-311/18 (2020).

Schrems v. Data Protection Commissioner, CJEU, C-362/14(2015).

United States v. Warshak, 631 F. 3d 266 (6th Cir. 2010).