

隐私经济学研究进展^{*}

贾传昌 朱建明 高 胜

摘要:经济数字化的不断发展和数据处理技术的进步已引起经济学家对个人信息在生产中的作用产生极大关注。隐私经济学是隶属于信息经济学的一个新兴研究领域,它关注一类特殊资源(个人信息)的配置,是运用经济学基本原理与方法来分析和解释隐私现象或问题的一门交叉学科。本文首先介绍隐私的概念及其经济价值,强调隐私概念的动态演化特征和隐私经济价值的异质性。其次,本文探讨共享个人数据的决策过程,分析什么因素助推了个人信息的披露行为以及隐私悖论存在的假设条件。再次,本文分别从数据确权、信息不对称、价格歧视、数据二次使用、数据外部性、隐私保护与规制等方面讨论隐私造成的消费者福利效应,并对隐私导致数据市场失灵的机制进行分析,总结隐私监管的经济影响,重申监管应该关注的具体隐私问题。最后,本文提出了隐私经济学研究存在的一些不足和未来拓展研究的方向。

关键词:隐私经济学 个人数据 隐私悖论 数据市场 消费者福利

一、引言

隐私一直是政策和经济辩论中敏感而热门的话题(Jones & Tonetti, 2020; Garratt & Van Oordt, 2021)。隐私经济学是隶属于信息经济学的一个新兴研究领域,但目前关于隐私经济学的定义尚未统一。早期的隐私经济学分析侧重于个人信息市场的效率(Stigler, 1980; Posner, 1981; Varian, 1996)。近期的一些学者关注保护和披露个人信息的经济价值(Acquisti et al, 2016)以及个人数据在市场中的作用(Cecere et al, 2017)。Acquisti et al(2016)认为,从本质上讲,隐私经济学涉及与个人、组织和政府之间在公共与私有领域相关的权衡取舍。并且,经济学家对隐私的关注主要集中在信息方面,即保护或共享个人数据所产生的权衡。Cecere et al(2017)也认为,隐私经济学旨在分析个人、企业和政策制定者在个人数据起关键作用的市场中如何相互作用。

当前,我国正处于数字化转型、数字经济快速发展的时期,越来越多的经济活动由数据驱动,数据已成为数字经济时代的关键生产要素。2020年中国数字经济规模达到39.2万亿元,占GDP比重达38.6%。2021年中国数字经济规模进一步扩大至42.4万亿元^①。《“十四五”数字经济发展规划》明确提出,到2025年,数字经济核心产业增加值占GDP比重预期达到10%。数据表明,我国数字经济规模不断扩张、贡献不断增强。另一方面,数据所带来的商业价值和利益激励越来越多的组织利用电子商务平台、社交媒体、移动应用和可穿戴设备等手段收集用户个人数据,往往表现为个人信息被过度收集。特别是美国的谷歌、亚马逊和脸书等独角兽互联网平台,以及中国的京东、腾讯、阿里巴巴等大型互联网企业的崛起,使得个人数据的收集和商业使用达到了前所未有的水平。从浏览、搜索历史到位置轨迹数据再到社交媒体活动,个人信息收集已渗透到人们生活的方方面面(Argenzi-

^{*} 贾传昌、朱建明、高胜,中央财经大学信息学院,邮政编码:100081,电子邮箱:chuanchang@163.com, zjm@cufe.edu.cn, sgao@cufe.edu.cn。基金项目:国家重点研发计划项目(2017YFB1400700);国家自然科学基金面上项目(62072487)。感谢匿名审稿人的修改建议,文责自负。

^①数据来源:《中国数字经济发展白皮书2021》。

ano & Bonatti, 2021)。

从现实背景看,2019年美国皮尤民调显示,个人对隐私的担忧正在上升,81%的受访者表示“公司收集有关他们数据的潜在风险超过了收益”。2020年Ghostery发布的一项研究显示,出于统计或广告目的,在全球范围内,谷歌保留了对所有网站80.3%的跟踪覆盖率^①。数字革命以及互联网已从初期乌托邦式的美好愿景演变成了赤裸裸的监视资本主义(Zuboff, 2019)。同时,用户为了获得便利和更好的服务,不断向互联网等平台共享个人信息,往往表现为个人信息的过度披露。据《2021年全国网民网络安全感满意度调查总报告》显示,仍有26.62%的网民认为网络个人信息保护不太好或非常不好,特别是在社交应用、电子商务和网络媒体等领域。个人信息的过度收集和过度披露为隐私安全埋下了隐患,不但容易造成自我信息泄露,而且还危及他人隐私(Acemoglu et al, 2019),也为第三方平台泄露提供了机会。数据泄露使电子商务等企业陷入高度的商业风险,也造成了严重的经济损失。根据IBM Security《2021年数据泄露报告的成本》显示,在新冠肺炎大流行期间,数据泄露成本创历史新高,2021年给企业造成的平均成本增加到424万美元,高于2020年的386万美元^②。

从政策背景看,欧盟《通用数据保护条例》(General Data Protection Regulation, GDPR)首次在法律上明确个人数据是个人资产,并要求企业使用个人数据需征得用户同意,即遵循“知情—同意”框架。美国《加州消费者隐私法案》(California Consumer Privacy Act, CCPA)则建议在收集和使用个人数据方面给予消费者更大的控制权。在国内,《中华人民共和国数据安全法》(以下简称“数据安全法”)也规定任何组织、个人收集数据应采取合法、正当方式。《中华人民共和国个人信息保护法》(以下简称“个人信息保护法”)作为中国首部针对个人信息保护的专门性立法再次明确了不得过度收集个人信息。2022年1月4日,中央网信办官网公布了《网络安全审查办法》《互联网信息服务算法推荐管理规定》两份重要文件,明确规定掌握超过100万用户个人信息的网络平台运营者赴国外上市必须向网络安全审查办公室申报网络安全审查。这些数据政策的宗旨在于遏制个人信息被滥用,保护个人隐私和数据安全。伴随相关法律、法规的出台,市场营销中的隐私环境已发生巨大变化,势必给互联网企业带来新的挑战。

综合现实和政策背景看,隐私仍然是一个亟待解决的问题。外部隐私环境的变化势必对消费者和企业产生冲击,特别是在经济方面。对于如何合理地配置宝贵的个人信息资源,消费者、企业和政府也可能需要重新考虑相关的权衡取舍:(1)消费者在保护和披露(或共享)个人信息之间的权衡;(2)在数据市场中,企业在隐私损失和数据效用之间的取舍;(3)政府立法在确保消费者隐私安全的同时还要不破坏企业的创新能力,而研究稀缺资源的合理配置是经济学的核心问题。长期以来,经济学家一直对了解个人信息披露的经济价值和后果以及共享个人数据的决策过程感兴趣(Acquisti et al, 2016)。鉴于此,本文对隐私经济学的研究进展做一评述。

二、隐私的概念及其经济价值

(一)什么是隐私?

“隐私”一词通常出现在法律、哲学、心理学、社会学和信息科学中。然而,对于隐私究竟是什么?学者们并没有形成广泛的共识。在操作上,隐私仍然是一个模糊的概念,人们很难给出明确的定义。例如,对于不同的人,隐私可能意味着不同的事情(Posner, 1981; Acquisti et al, 2016)。

隐私一词最早可以追溯到1890年《哈佛法学评论》上发表的一篇题为《隐私权》的文章中。Warren & Brandeis(1890)将隐私定义为“不受打扰的权利”,这被公认为隐私概念的首次出现。随后,关于隐私定义的哲学争论在20世纪下半叶变得异常突出,特别是隐私的概念随着信息技术的显著进

^①数据来源:<https://www.ghostery.com/blog/tracking-the-trackers-2020-web-trackings-opaque-business-model-of-selling-users>。

^②数据来源:<https://www.ibm.com/security/data-breach>。

步而不断演变,将其推置公众辩论的前沿。通过对现有文献的梳理,发现主要有如下五种隐私定义。

1. 将隐私定义为权利。隐私本身被视为一种内在权利,特别是作为“不受打扰的权利”(Warren & Brandeis, 1890)。当前,许多国家的法律将隐私视为一项必须受到保护的基本人权(Solove, 2008)。基于这种隐私概念,个人信息的处理必须受到限制。

2. 将隐私视为商品。在数字时代,个人信息被认为是一种新的商品(Spiekermann et al, 2015)。基于商品的定义是指用户将其个人信息作为无形资产进行交易(Xu & Gupta, 2009)。一些学者认为隐私不仅是个人的一项重要权利,也是一种中间产品(Farrell, 2012)或最终商品(Acquisti et al, 2016)。此外,Fairfield & Engel(2015)主张从公共品的视角来研究隐私。隐私的商品化为研究个人信息价值提供了重要基础。

3. 将隐私定义为对信息的控制。关于隐私的最主要理论之一是个人信息控制理论。例如,Westin(1968)认为隐私是“对自我访问的选择性控制”。Flaherty(1989)则明确地提出了将隐私作为信息控制的想法,并且将“数据保护”发展为隐私的一个方面,这一概念为公平信息实践(FIP)奠定了基础。类似地,Acquisti et al(2016)认为隐私不是共享的对立面,而是对共享的控制。

4. 将隐私定义为状态。隐私还可以被视为一种能够实现自主的状态,这是一个与人格密切相关的概念。Westin(1968)通过孤独、亲密、匿名和保留四种状态来定义隐私。类似地,Laufer & Wolfe(1977)将一般隐私概念化为一种情境概念(状态)。需要指出的是,不同状态的隐私可能影响我们与他人的互动方式。

5. 将隐私作为集体规范。Shaeffer & Keever(2021)认为个人数据在孤立的情况下并没有什么价值,只有与其他人所做、所说和喜欢的信息结合在一起时才变得更有价值。个人数据汇总而成的大数据不是个人财产,而应视为集体规范,因此他们提议从集体的角度对个人数据重新定义。

综合以上学者观点可知,统一的隐私定义尚不存在。隐私已通过权利、商品、控制、状态和集体规范等多种方式概念化。为了厘清现有文献中隐私的概念,Smith et al(2011)采用基于价值和基于同源(cognate-based)的定义来归纳隐私概念。其中,基于价值的定义是将隐私视为商品或社会道德价值体系中不可或缺的一项人权。而基于同源的定义主要是把隐私等同于具有共同词源的词,例如,把隐私看作一种控制或状态。结合 Smith et al(2011)的定义方法,可以对上述五种隐私的定义进行归纳,如表 1 所示。

表 1 隐私定义的分类

定义方法	具体分类	特征	相关文献
基于价值	隐私作为一项权利	隐私是一项基本的人权	Warren & Brandeis(1890)
	隐私作为一种商品	隐私是可以交换感知利益的商品	Xu & Gupta(2009) Farrell(2012) Spiekermann et al(2015) Fairfield & Engel(2015) Acquisti et al(2016)
基于同源	隐私作为控制	隐私等同于对访问和信息等的控制	Westin(1968) Flaherty(1989) Acquisti et al(2016)
	隐私作为一种状态	隐私等同于某种状态,影响我们与他人的互动方式	Westin(1968) Laufer & Wolfe(1977)
	隐私作为集体规范	隐私应被视为一种集体规范,而非个人财产	Shaeffer & Keever(2021)

另外,也有学者将隐私划分为不同的维度来尝试澄清隐私的定义和范围。例如,Dienlin & Trepte(2015)将隐私区分为信息隐私、社会隐私和心理隐私三个维度,然后针对不同的隐私维度进行研究。本文认为,如果要界定清楚隐私的概念,首先应明确其研究的范围和维度,然后结合 Smith et al(2011)的基于价值或基于同源的定义进行界定。例如,在隐私经济学中(而不是法律或其他领

域中)诠释信息隐私(而不是心理、物理或社会隐私等)的概念,最后,基于价值或基于同源的定义来明确信息隐私的含义。信息隐私已成为隐私领域学者们的前沿研究焦点,隐私经济学主要关注信息隐私相关的研究。

(二)隐私的经济价值

隐私经济学始于“个人数据商品化为可交易的资产”(Spiekermann, 2015)。个人信息在经济价值作为商业、法律和政策领域的客观评估指标具有重要意义(Lim, 2021)。实际上,很多有价值的数据集本质上是个人。个人数据越来越被视为商业资产,甚至被喻为现代经济中的“新石油”。虽然大多数经济学家对个人隐私具有经济价值早已达成共识,但是隐私通常与产品或服务捆绑在一起进行销售,这导致很难衡量隐私的具体经济价值。

尽管估计隐私的经济价值面临诸多挑战,然而,长久以来,经济学家一直对如何估计隐私的经济价值感兴趣,并且一些学者已在不同的场景中对隐私的经济价值进行了估计。Taylor(2004)认为,客户信息的价值来源于互联网企业识别消费者并向他们收取个性化价格的能力。隐私经济价值的货币化主要体现在两个方面:一方面,披露个人信息时,用户愿意接受的最低价格(即WTA);另一方面,保护个人信息时,用户愿意支付的最高价格(即WTP)。

1. 用户愿意以最低价格出售个人信息的相关实证研究。Carrascal et al(2013)在田野实验中,采用反向二价拍卖研究了消费者在网上浏览时如何重视个人身份信息。研究表明,用户倾向于重视他们的线下隐私,并且愿意以25欧元(中位数)披露他们的年龄和地址信息,以7欧元(中位数)分享他们的在线浏览历史。类似地,Cvrcek et al(2006)估计了向第三方披露位置数据的价值。结果发现,用户愿意以每月43欧元的价格放弃他们的位置数据。Beresford et al(2012)通过田野实验对电子商务交易中消费者的出生日期和月收入披露进行了估计,结果显示消费者的WTA相当于1欧元折扣。

2. 用户愿意支付最高价格保护个人信息的相关实证研究。Potoglou et al(2015)、Krasnov et al(2009)和Hann et al(2007)通过离散选择实验分别对避免共享和存储、防止二次使用个人数据、避免个性化广告以及隐私增强服务以保护隐私的WTP进行了估算。研究发现,为了避免与第三方共享个人数据的WTP为每笔交易5.57英镑,用户愿意支付2.68英镑避免在线零售商存储其个人数据(Potoglou et al, 2015)。而防止不当访问和二次使用个人信息的WTP范围在30~45美元之间(Hann et al, 2007)。在使用人口统计信息的在线社交网络中,避免个性化广告的平均支付意愿为每年14~17欧元,关注隐私的用户愿意为相同的服务每年支付23~28欧元(Krasnov et al, 2009)。Egelman et al(2013)通过田野实验对隐私增强应用和Facebook数据可移植性的WTP进行估计发现,对于请求最少个人数据应用程序的WTP,在注重隐私的参与者中为1.5美元(25%),当支付超过0.99美元时,80%的参与者将放弃个人数据的保护。

综合上述研究可知,个人信息不是同质产品。不同类型个人数据的经济价值也不同,即使是同一类型个人数据的经济价值也是因人而异。值得注意的是,现有隐私经济价值的研究主要关注人口统计方面的类型信息,通过实验等研究方法对客户在披露隐私时WTA和保护隐私时WTP进行比较,而实际上,不同类型的个人数据可以揭示不同的个人信息。本文认同Acquisti et al(2016)的观点,即隐私的经济价值不是单一价值的统一概念,而是与上下文相关,并且因不同类型的数据而有所不同。尽管隐私的经济价值呈现出典型的异质性,但仍可能存在潜在的个人隐私偏好。本文只探讨隐私的经济价值,并不是说隐私的政治价值等其他价值不重要,而是隐私经济学主要关注隐私的经济价值。

三、隐私披露行为的理论与实证研究

(一)个人信息披露成因相关理论与实证研究

一直以来,经济学家始终对共享个人数据的决策过程感兴趣。已有许多学者从不同理论与实证

方面研究和解释了为什么人们愿意披露(或共享)个人信息,有时甚至“乐此不疲”。这方面的文献大体可以分为两类,理性的披露决策以及非理性或有限理性的披露决策。

1. 理性的披露决策。相对于直觉、冲动的决策,人们可能更加理性,善于推理计算。作为最流行的信息隐私研究框架之一,隐私计算(privacy calculus)理论认为披露个人信息的意图总是基于理性的收益风险计算,即在收益与风险之间权衡。当个人预期收益将超过隐私损失的风险时,则披露个人信息以换取社会或经济利益(Trepte et al, 2020)。例如,在移动场景中,Pentina et al(2016)研究发现,移动应用的使用主要受感知信息和社会效益的驱动。Wottrich et al(2018)在一个实验环境中也证明了隐私权衡的存在。近期的实证研究发现,在确定满意度时,感知利益比感知风险更重要,感知利益通过满意度间接影响访问个人信息的意愿(Najjar et al, 2021)。资源或社会交换理论也有类似的观点,认为由于个人的愿望和需要,他们试图理性地与他人交换资源。例如,最近的实证研究表明,互惠交换强烈影响在线购买中披露个人数据的意愿(Urbonavicius et al, 2021)。

2. 非理性或有限理性的披露决策。人们在做决策时,受到启发式、认知偏见和知识能力限制等多种因素影响,往往表现为非理性或有限理性(Kokolakis, 2017)。自我披露可以理解作为一种认知决策,情感在人类判断和决策中的作用不容忽视(Najjar et al, 2021)。根据情感启发式理论,人们用情感标记行为、对象或事件,然后参考他们的“情感池”进行决策和行为。被激活的情感会影响人们对行为的认知评估(Yu et al, 2015)。作为社会人,一个人的社会环境对他的隐私决策和行为有显著的影响(Beldad & Kusumadewi, 2015)。例如,Acquisti et al(2012)通过现场实验表明,披露个人信息存在羊群效应,羊群行为影响人们披露敏感信息的倾向。Trepte et al(2020)在社交网站(SNS)环境也验证了这一结论。最近关于解释水平和信息边界理论(通信隐私管理理论)的文献也有新的见解。Bandara et al(2021)在一项问卷调查中发现,心理距离能够解释隐私行为并调节隐私关注与隐私行为之间的关系,但被授权的消费者的隐私行为并没有显著变化。在个性化广告场景中,Zhu & Kanjanamekanant(2021)通过问卷调查研究了隐私边界对社交媒体广告态度和购买意愿的影响。结果发现,基于内部数据源的个性化广告、可感知的人格化和共同所有权与可感知的隐私呈正相关,从而导致更好的广告态度和更高的购买意愿。

综合以上分析可知,隐私决策依赖于具体情境,信息披露决策是一个结合了理性和情感因素的复杂过程(Najjar et al, 2021)。现有文献已将隐私研究扩展到各个方向,隐私计算理论、资源或社会交换理论、情感启发式理论、解释水平理论、通信隐私管理理论以及信息边界理论等都能很好地解释个人信息的披露行为。而且,最近一些学者通过实证分析引入新的隐私前因(antecedents),再次验证了这些理论的有效性。当前,现有研究主要使用两种流行的结构之一(Concerns for Information Privacy, CFIP)或(Internet Users' Information Privacy Concerns, IUIPC)衡量用户的信息隐私问题(Smith et al, 1996; Malhotra et al, 2004)。隐私关注的实证分析主要通过“前因—隐私关注—结果”(APCO)宏观模型来研究(Smith et al, 2011)。考虑到 APCO 模型存在对外部刺激的反应会导致深思熟虑的分析,从而导致完全知情的隐私相关态度和行为问题,Dinev et al(2015)将行为经济学和认知心理学的变量(如启发式和偏见)引入模型,并提出了增强的 APCO 模型。该模型强调了上下文和情境对隐私决策的影响,为研究隐私问题提供了一个新的框架。

(二)关于隐私悖论的争论

长期以来,隐私学者认为人们会做出合理的隐私披露决定。Westin(1968)更是用“隐私实用主义者”来形容这些理性人。直觉上,隐私具有经济价值,应该受到重视。事实上,人们确实声称关注隐私(Madden & Rainie, 2015),然而,他们表现出来的态度和行为却背道而驰,这种隐私态度或偏好与实际或实验室行为相背离的现象称为“隐私悖论”(Barnes, 2006; Acquisti et al, 2016)。隐私悖论现象对隐私偏好的一致性提出了挑战。人们不禁会产生疑问,我们真的关心自己的隐私吗?如果关心,为什么个人信息的声明价值和披露价值之间存在差异?为此,已有许多研究试图揭开隐私悖论的神秘面纱(Chen et al, 2021; Glasgow et al, 2021),但学者们对于隐私悖论是否存在尚存分歧。

1. 支持隐私悖论存在的研究。基于自我决定理论, Hew et al(2017)通过调查问卷,采用 PLS-SEM 方法,在智能旅游背景下确认了隐私悖论现象。Athey et al(2017)利用来自麻省理工学院数字货币实验的现场实验数据,调查了消费者在面临通知和选择时的行为扭曲,发现了数字隐私悖论。Aleisa et al(2020)使用访谈、问卷和观察等混合方法证实了正在兴起的物联网领域存在隐私悖论,进一步拓展了研究的范围。Arpetti & Delmastro(2021)通过实证调查对消费者的隐私决策进行分析发现,意大利也出现了声明意图和个人实际行为之间的矛盾。Glasgow et al(2021)基于假设的叫车服务,通过离散选择实验检验调查响应偏见导致隐私悖论的证据。结果显示调查设计之间的差异在统计学上不显著,没有证据支持受试者内部设计可能导致隐私悖论的调查反应偏差。

2. 挑战隐私悖论存在的研究。隐私实际上是一个高度依赖于上下文并随时间可变的概念(Kokolakis, 2017),因此,一些学者对隐私悖论存在性提出质疑。Mothersbaugh et al(2012)研究在线服务环境中的披露前因发现,隐私关注对整体披露没有影响,但对较高敏感的信息有预期的负面影响,隐私悖论可能是由于未能考虑到信息敏感性所导致。Dienlin & Trepte (2015)将隐私区分为信息隐私、社会隐私和心理隐私三个不同维度,通过在线调查问卷,结合计划行为理论(TPB)展开研究,结果表明,在线隐私关注与特定隐私行为的相关性不显著。使用隐私态度、隐私关注和隐私意图可以充分解释隐私行为,社交网络中的用户行为并不像人们认为的那样自相矛盾,隐私悖论只不过是“过去的遗迹”。Chen et al(2021)针对个人数据共享与隐私担忧相关的问题,对支付宝小程序用户进行了为期一年的调查。结果表明,46%的人表示非常关心隐私,39%的人表示关心,只有15%的人不关心。在一年时间里,“非常关心”隐私的用户平均访问了16.3个小程序,授权了其中11.3个小程序,并拒绝了将近25%的数据共享请求。这些“非常关心”隐私的用户没有因为盲目授权所有请求而放弃对其数据隐私的积极保护。通常,隐私悖论研究中涉及的行为是人们在非常特定的环境中做出的风险决策,而相对风险和客观风险都会影响消费者的隐私抉择(Adjerid et al,2018),Solove (2021)认为隐私悖论只不过是错误逻辑创造的神话。

现有文献对隐私悖论现象的解释主要是分析阐明隐私态度和隐私行为之间的分歧,重点研究隐私悖论存在的假设条件,主要体现在隐私计算理论、社会交换理论、决策中的认知偏见和启发式、有限理性和信息不对称条件下的决策以及量子同态理论等五个研究领域(Kokolakis,2017)。最近有关注意力和数据外部性的研究为隐私悖论的解释提供了新的见解。预计到2025年,全球每天生成的数据量将达到463艾(1艾=2⁶⁰)字节,海量大数据和多屏幕使得用户分心几乎无处不在。注意力的减少可能决定消费者对个性化隐私悖论的评估(Cloarec, 2020)。通常,在存在负数据外部性的情况下,消费者将面临过度的数据共享,个人信息的价格也将进一步被压低(Bergemann et al,2020; Ichihashi, 2020b),而保护个人信息也变得更加困难。消费者在面对可忽略的边际隐私成本和较高的隐私保护成本时,以非常低的价格放弃个人数据看来也是合情合理的(Athy et al, 2017)。有关隐私悖论更早的讨论可参考Barth & De Jong (2017)和Kokolakis(2017)的研究综述。

四、隐私与消费者福利相关的研究

个人数据市场的分散促使人们对在线消费者信息的福利效应越来越感兴趣(Argenziano & Bonatti,2020)。当前,数据权属界定不清已成为数据要素化的最大制度障碍之一(熊巧琴和汤珂,2021)。在数据丰富的数字世界中,个人用户和数据收集平台之间的信息不对称几乎是一种自然状态(Martens,2021)。而这些固有的信息不对称似乎无法消除,这是数据驱动经济的“原罪”(Ciuriak, 2019)。由信息不对称导致的价格歧视对消费者福利的影响并不明确(Gu et al,2019; Bergemann et al,2020)。我们应该认识到任何政策对消费者福利的影响都具有两面性(Argenziano & Bonatti, 2021)。随着新技术的引入,消费者担心他们的数据被收集并用于他们毫不知情的目的,未经授权的二次使用产生显著的负外部性(Noam,1997)。目前,数据外部性的福利影响研究仍然是学者们近期关注的热点问题(Bergemann et al,2020; Fainmesser,2021)。

(一)数据确权

互联网的兴起伴随着关于如何使用和控制数据的激烈辩论(Jones & Tonetti, 2020; Markovich & Yehezekel, 2021)。数据权属界定不清已成为数据要素化的最大制度障碍之一。

根据科斯逆定理,当存在交易成本时,不同的权利界定会带来不同效率的资源配置。Taylor (2004)考虑到了这种产权安排,调查了消费者隐私和电子零售中的客户信息市场,研究在客户信息的保密制度和披露制度两种情况下的福利效应,并在披露制度的背景下讨论天真和成熟消费者的不同情形,认为福利比较在很大程度上取决于消费者是否预期名单的销售和需求弹性。类似地,Dosis & Sand-Zantman(2019)研究了使用数据时产权对市场结果的影响,发现数据归属企业还是消费者所有取决于数据对企业的总体价值以及消费者能够将其数据货币化的程度。Ali et al(2020)在垄断和竞争环境下进一步调查了让消费者控制自己数据的经济影响。研究表明,消费者是否能从信息控制中获益,取决于消费者披露信息的技术与市场竞争程度之间的微妙互动。Jones & Tonetti(2020)也关注产权,但更强调数据的非竞争性。他们考虑到企业拥有数据的缺点——过度使用数据而不能充分尊重消费者隐私和担心创造性破坏而囤积数据,研究了企业拥有数据和消费者拥有数据的不同情景,并且比较了这两种数据产权制度安排下的消费者福利。分析表明,赋予消费者数据产权可以产生接近最优的分配,均衡福利为最优福利的99%。而当企业拥有数据时,均衡福利仅为最优福利的93%。然而,Bergemann et al(2020)认为赋予消费者对其数据的控制权不足以实现信息的有效使用。

(二)信息不对称

信息不对称是数字平台经济中的一个现实(Martens, 2021)。大数据中固有的信息不对称似乎无法消除,这是数据驱动经济的“原罪”(Ciuriak, 2019)。平台可以利用这种信息不对称来促进互动,增加消费者福利(Martens, 2021),然而,大量的信息不对称也会增加消费者的搜索成本或对消费者进行价格歧视,降低消费者福利,甚至导致非最优结果的市场失灵(Lancieri, 2021)。

信息不对称是数字隐私市场失灵的重要来源。数据共享经常被“吹捧”为克服信息不对称和最大化社会福利的一种手段(OECD, 2019)。所以一些学者认为市场机制产生的数据共享太少而不是太多(Varian, 1996; Jones & Tonetti, 2020),这与“芝加哥学派”的观点如出一辙。Stigler(1980)和Posner(1981)认为个性化数据的增强使用提高了效率和福利,因为信息不对称减少了。然而,第三方跟踪的做法扩大了个性化数据收集和使用的信息不对称问题,对消费者福利造成负面影响的可能性增加。数据市场的复杂性进一步加剧了信息不对称和市场集中度的担忧(Lancieri, 2021),反垄断机构似乎难以评估因数据集中度增加或并购对消费者造成的损害(Schoch, 2020)。Eeckhout & Veldkamp(2022)认识到增加数据不对称有两个互异的福利效应:一方面,增加了市场力量,可能造成福利的无谓损失;另一方面,拥有更多信息的企业生产更多,可以降低风险的负效用。在数字时代,消费者实际面临着信息过载(Acemoglu et al, 2019),不断寻求分配稀缺注意力的最佳方法(Jin & Wagman, 2021)。

(三)价格歧视

隐私经济学的核心问题是企业可能会利用消费者数据进行价格歧视(Ali et al, 2020),这可能会对消费者福利构成威胁,问题的根源在于价格歧视所利用的信息不对称。最近的研究和政策报告强调,数据驱动的价格歧视对消费者福利的影响并不明确(Montes et al, 2019; Bergemann et al, 2020)。

Gu et al(2019)关注于竞争企业在价格竞争中领先的动机。研究表明,当确定了足够的消费者份额时,价格歧视的能力会成为一项重要的战略资产。个性化定价通常具有促进竞争和提高福利的效果,但只适用于价值非常大的消费者。在某些情况下,即使是标准的、完美的价格歧视,也会对消费者和整体福利造成严重损害。Montes et al(2019)研究了信息和隐私在市场中的作用,调查了价格歧视对价格、利润和消费者剩余的影响。Bonatti & Cisternas(2020)将棘轮效应的连续时间模型

嵌入到信息设计框架中,研究了将购买历史汇总为用于三级价格歧视的评分的福利后果,基于购买历史的价格歧视明确地伤害了天真的消费者,但可以使战略消费者受益。Ichihashi(2020a)讨论了卖家在承诺制度和无承诺制度下在线购物市场消费者隐私的福利和价格影响,研究表明,在承诺不使用消费者的信息进行定价时,可以诱导消费者披露更多的信息,卖家可能会利用这些信息对消费者进行价格歧视以获得更高的收益,而消费者的境况会变得更糟。当卖家承诺保留一些信息时,消费者的境况会更好。此外,Bergemann et al(2020)将隐私问题内部化,以量化数据中介对下游福利的影响。当数据中介将数据出售给生产者时,可以实现更准确的价格歧视,这降低了所有消费者的福利。

(四)数据二次使用

随着新技术的引入,消费者担心其数据被收集并用于他们根本不知道的用途。二次使用的可能性会对个人信息在未来如何使用产生恐惧和不确定性,从而产生一种无力感和脆弱感。未经授权的数据二次使用通常会产生显著的负外部性(Noam, 1997),影响消费者福利。

Varian(1996)开创性地区分了互联网企业对个人信息的第一次使用和第二次使用。Taylor(2004)认为在未经用户同意的情况下,第三方使用或在同一企业内二次使用个人数据似乎不合法,这种行为对消费者的福利是递减的。Akçura & Srinivasan(2005)使用一个理论模型也证实了二级市场会导致消费者福利的急剧下降。Fairfield & Engel(2015)研究发现,共享数据具有外部性,企业可能会在个人毫不知情的情况下再次使用个人数据。例如,剑桥分析数据丑闻导致消费者在未经同意的情况下滥用其个人数据,这可能造成消费者隐私损失和福利降低。Jentzsch(2017)对个人数据的二次使用进行了福利分析,并使用垄断销售者模型研究了匿名、披露和临时三种不同隐私制度下的消费者福利。从模型中获得的经验是,政策制定者应该牢记数据保护法规转移了市场参与者的产权和补偿。另外一些隐私评估有关的文献也关注数据的二次使用,Preibusch(2013)认为二次数据使用是隐私评估的主要驱动因素。消费者对信息隐私的关注主要体现在对个人信息收集的关注、对个人信息的内部和外部未经授权的二次使用、个人信息中的错误以及对个人信息的不当访问几个方面(Smith et al,1996)。

(五)数据外部性

Ichihashi(2021b)认为企业和消费者如何分配由数据创造的剩余取决于数据的外部性。数据外部性是由于个人数据的披露而产生的影响,可能是积极的影响(正的数据外部性),也可能是消极的影响(负的数据外部性)。正的数据外部性提高福利,而负的数据外部性降低福利(Varian 1996; Acquisti & Varian 2005)。数据驱动的外部性的福利影响工作仍然是学者们最近讨论的热点问题(Bergemann et al,2020; Fainmesser et al,2021)。

数据外部性在个人数据的社会过度传播中的作用一直是 Choi et al(2019)关注的焦点。他们重视消费者方面的信息外部性,研究了信息外部性如何导致数据定价过低以及社会上过度的数据收集的问题。而且,他们提出了一个基于信息外部性概念的隐私模型,在不存在信息外部性的情况下,每个消费者都可以通过选择不消费来避免隐私成本。然而,当存在负的隐私外部性的时,特别是隐私泄露危及未披露信息的消费者时,这些消费者的福利将遭受损失。类似地,Acemoglu et al(2019)在考虑存在数据外部性的情况下对数据市场进行建模,研究证明数据的外部性压低了数据的价格,而低迷的价格导致了过度的数据共享,并可能进一步造成大量的隐私损失和福利降低。Bergemann et al(2020)也发现数据外部性普遍存在。个人数据的主要特征是其社会方面,这些个人数据实际上是社交数据。数据的社会性质产生数据外部性,其符号和大小取决于所获得信息的最终用途。赋予消费者对其数据的控制权可能制约信息的有效使用。

(六)隐私保护与规制

在线隐私保护已成为全球关注的主要问题。近期频繁发生的诸如剑桥分析数据丑闻、大数据杀熟等数据泄露事件更凸显了隐私问题。在此背景下,监管机构近年来出台了一系列隐私法规,例如,

GRPR、CCPA 和个人信息保护法皆在保护个人隐私和避免个人数据被滥用。虽然隐私保护为消费者带来了好处,但它也通过限制个人数据的使用而增加了成本。并且,数据保护策略也是一项成本高昂的投资(De Corniere & Taylor, 2020)。由此可见,任何政策对消费者福利的影响都是双重的(Argenziano & Bonatti, 2021)。

隐私保护的剩余工具是政策干预(Acquisti et al, 2020)。诸多研究表明,加强数据保护的 policy 可能会增加进入企业的成本以及消费者的转换和采用成本,增加进入壁垒(Jia et al, 2019)。Fainmesser et al(2021)讨论了监管机构应采取什么行动来保护消费者隐私和最大限度地提高社会福利。结果表明,当数据收集策略受到限制时,数据保护的增加降低了隐私成本。Johnson et al(2020a)估计了隐私政策对在线展示广告行业的财务影响,结果表明,选择加入政策或跟踪禁令会大大减少福利,但选择退出政策几乎没有影响。当竞争足够激烈时,严格禁止收集和使用个人数据的法规会降低效率和消费者福利(Hoffmann et al, 2020)。Argenziano & Bonatti(2021)研究了异质企业之间的数据联系,并分析了三种不同形式的强制消费者同意措施的影响。研究发现,相对于纯自愿同意的情况,增加自愿同意要求提高了消费者福利,但禁止歧视会减少这种福利,任何政策对消费者福利的影响都是双重的。同样,Jullien et al(2020)也认为很难通过改善消费者福利的方式来规范隐私保护。例如,提高隐私政策透明度并让消费者更好地控制其个人信息的政策对消费者福利的影响是不确定的。

影响隐私和消费者福利之间关系的原因是多方面的,数据确权、信息不对称、价格歧视、数据二次使用、数据外部性以及隐私保护与规制等都是重要的因素。消费者剩余和社会福利在这些方面也不是完全单调的,例如,福利在不对称信息的数量上并非单调(Jann & Schottmüller, 2020),针对消费者的政策可能会对平台的供应方产生意想不到的负面影响(Martens, 2021),即使是只要求消费者许可而不禁止收集和使用个人数据的监管也可能适得其反,甚至降低消费者福利(Hoffmann et al, 2020)。此外,数据经纪人(data brokers)策略(Ichihashi, 2021a)、诱惑(Liu et al, 2020)和成瘾性平台(Ichihashi & Kim, 2021)等同样影响消费者福利。数据立法和监管机构需要在消费者隐私、社会福利和企业创新之间权衡取舍。

五、隐私、数据市场与监管

随着人工智能、大数据、移动互联网和物联网等技术的普及和快速发展,企业和其他组织对个人数据的收集、合并、清洗、分析、购买和出售达到了前所未有的规模,并由此催生了许多新兴的数据市场。例如,基于查询定价的数据市场 Google Bigquery,基于数据定价的数据市场 Dawex、Bloomberg 和 SafeGraph。由于个人信息是一种具有非竞争性和非排他性的经济商品,使得数据市场更容易形成由垄断市场(Martens, 2021)、信息不对称(Bergemann et al, 2020)、数据外部性(Acemoglu et al, 2019)和缺失市场(Economides & Lianos, 2021)等特征导致的市场失灵。最近的剑桥分析数据丑闻、大数据杀熟以及滴滴赴美上市事件进一步凸显了隐私问题。个人数据新市场的兴起以及频繁的数据泄露事件吸引了监管机构的注意,政策制定者试图通过隐私立法与监管来平衡消费者隐私安全与企业创新之间的紧张关系。

(一) 隐私与数据市场

数据市场是促进数据买卖的在线交易场所或商店,销售的常见数据类型包括商业情报、广告、个人信息以及研究和市场数据等。从经济角度看,数据交易市场可能是提供和使用数据的最有效方式(Budzinski et al, 2021)。实际上,关于提供数据市场的建议并不新鲜,早在 20 世纪 90 年代中期,Laudon(1996)就提议建立一个信息市场。“芝加哥学派”认为个人信息市场与传统商品和服务市场一样有效(Posner, 1981; Stigler, 1980)。然而,个人信息不同于传统经济商品,是一种具有非竞争性、非排他性和社会性等特征的经济商品。这些特性使得数据市场更容易形成由垄断市场、信息不对称和数据外部性等导致的市场失灵。

1. 垄断市场。一方面,现代信息通信技术的快速发展使得数据收集、存储和分析的成本不断下降,同时降低了信息披露的成本;另一方面,数据驱动的科技企业通常受益于网络效应、规模经济和范围经济的正反馈循环(Schoch,2020; Martens,2021)。例如,人工智能和机器学习的兴起进一步扩大了数据聚合的规模经济和范围经济。数据聚合中的规模经济和范围经济是正外部性的来源(Gans,2020)。再者,数据可以在一个市场收集并在另一个市场重复使用。Martens(2021)探讨了数据市场的经济学,并且区分了由数据重用与聚合所产生的范围经济。这些方面的因素激励了越来越多的企业将数据置于其商业模式的核心,以数据为中心的战略改变了现有的商业模式(Lies,2019)。市场倾向于垄断,数据的非竞争性增强了数据市场的市场集中度,可能导致“赢者通吃”的局面(Hill et al,2015)。此外,数据驱动的网络效应加强了平台的垄断市场地位(Martens,2021)。一些互联网企业为了追逐竞争优势,利用锁定效应、用户黏性等方式,可能在数据市场中滥用支配地位。例如,平台实施“二选一”,不仅损害了竞争者的利益,而且减少了消费者选择的机会,最终导致市场的低效率。

2. 信息不对称。真实世界的数据市场与Laudon(1996)最初关于信息市场的设想非常相似,但是又有着明显的不同——用户(数据主体)缺乏对他们自己个人信息的控制。具体地说,数据收集者而不是用户自己拥有他们的个人数据。消费者通常在关于何时被收集数据,出于何种目的以及产生何种后果的信息上处于不对称的位置(Acquisti et al,2016)。例如,参与Google互联网搜索和Facebook服务的每个人都在以近乎零的价格提供他们的个人数据,“如果你不是客户,你就是产品”,这似乎适用于大部分的数字经济,用户以此为代价换取免费的搜索和社交服务,而这些数据的具体用途及其对用户产生的经济后果都是不透明的。平台将利用这种信息不对称作为自己的优势细分消费者市场,创建更准确的消费者群体,对其进行价格歧视(Montes et al,2019; Bonatti & Cisternas, 2020),以攫取更高的利润。在大数据市场中,定价时更容易考虑每个消费者的隐私信息,个性化价格可以近似于一级价格歧视,消费者剩余将趋近于零。当大量的信息不对称增加消费者的搜索成本时,市场也会失败(Lancieri,2021)。

3. 数据外部性。非排他性商品原则上可能更具吸引力,因为它可能产生正的外部性,搭便车能够从中受益。但是,同时它也可能带来负外部性,导致数据安全问题(Gal & Ghose, 2005)。例如,在某些情况下,有关我的数据能够揭示你的一些特征(Acemoglu et al, 2019)。这意味着一个人共享自己的个人信息可能危及他人的隐私,给他人造成负的隐私外部性,Aridor et al(2020)通过一个自然实验的实证研究首次识别了隐私外部性。在考虑这种外部性的情况下,Acemoglu et al(2019)对数据市场进行建模,并证明数据的外部性会降低数据的价格,而且会带来低效率的大量隐私损失,甚至可能会导致数据市场崩溃。类似地,Choi et al(2019)也研究了数据外部性如何导致数据定价过低,并导致社会过度数据收集的问题。Bergemann et al(2020)还考虑了一种信息结构,其中,数据外部性使得私人成本大于社会成本,这可能造成数据共享效率低下。Ichihashi(2021b)更是提出了数据外部性经济学,描述了最大化消费者剩余和企业利润的数据外部性,并使用该结果解决一个信息设计问题。

在数据市场中,经济学家主要关注隐私损失和数据效用(准确性)之间的权衡(Abowd & Schmutte 2019)。一方面,消费者希望披露的数据最小化以获得需要的商品或服务;另一方面,企业渴望通过大数据对消费者构建精准用户画像,实现数据效用最大化,以获得高额利润。综合上述数据市场的特征与问题,我们应该认识到在获取和利用个人信息方面存在市场失灵。数据驱动的市场更容易出现因垄断市场、信息不对称和负的数据外部性等因素导致的市场低效率或无效率。此外,由于缺乏对个人数据的产权,数字经济似乎具有“缺失市场”的特征(Economides & Lianos,2021)。为了纠正数据驱动的市场失灵,设计有效的数据市场模型对于通过支持数据所有者和数据购买者之间的数据交易至关重要。Acemoglu et al(2021)和Bergemann et al(2020)将数据建模为信息,并探讨了数据市场是否有效。此外,制定相关的数据隐私政策,并对数据市场进行监

管也不可或缺。

(二) 隐私监管

信息资产的价值和监管一直是经济研究中的一项重要议题(Acquisti et al, 2016)。从经济角度看,监管机构需要对数据市场进行干预,以解决由数据驱动导致的市场失灵。从政策的角度看,政府需要制定相关的法律措施以保护个人隐私。特别是在网络环境下,个人隐私的隐私权是通过“知情—同意”原则来实现的(Solove, 2013)。进入数字经济时代,数据已成为新经济的重要生产要素,是互联网等企业赖以生存和创新的根本。数据安全监管是数据要素发展利用的前提和保障,监管机构一方面要确保消费者个人隐私安全;另一方面还要不破坏企业的创新能力。现有文献主要围绕数据市场是否需要监管以及隐私监管的结果和经济影响等方面展开研究。

由前文的分析可知,数据驱动的市场存在因垄断市场、信息不对称、负的数据外部性和缺失市场等因素导致的市场失灵。所以通过数据立法和监管来纠正市场失灵对数据市场进行有效治理是必不可少的。一个典型的案例是加密货币市场,由于早期缺乏监管,每年大约有 760 亿美元的非法活动涉及比特币,占比特币交易的 46%(Foley, 2019)。最近备受瞩目的剑桥分析数据丑闻、大数据杀熟定价以及“二选一”等事件进一步表明数据市场的监管势在必行。

监管市场透明度是各国政府和监管机构的一个重要政策问题(Martin, 2020)。Fast et al(2021)认为对数据市场进行监管干预是必要的,因为政策干预不仅可以提高透明度,还可以增强消费者对个人数据的控制。Betzing et al(2020)通过在线实验测试透明度如何影响用户做出知情决策,结果表明,当隐私政策被透明地披露时,人们对数据处理实践的理解有所提高。Acquisti et al(2017)和 Schaub et al(2017)认为,同意机制和数字用户界面的设计在塑造消费者的实际行为以及确定透明度监管的有效性方面发挥着至关重要的作用。此外,选择事前监管还是事后监管,或者两者兼而有之,也是监管机构需要考虑的问题。事前监管规定了处理个人数据的基本注意标准,降低了数据被滥用的可能性(Brown, 2016)。例如,近期颁布的数据隐私法规《通用数据保护条例》《加州消费者隐私法案》《个人信息保护法》赋予数据主体知情权、访问权、被遗忘权和反对对其数据进行某些处理的权利。Lam & Lyons(2020)的研究表明,GDPR 的知情同意降低了消费者为商业用途提供数据的意愿,这从某种程度上降低了数据被滥用的风险。Lefrere et al(2020)采用双差分(DID)方法估计 GDPR 对内容提供商的影响。结果表明,没有发现该法规对欧盟网站发布的内容量、社交媒体的平均参与度以及与此内容的互动程度产生负面影响的重要证据。事后责任制度赋予因滥用个人数据而受到伤害的个人对数据控制者采取行动的权利,这迫使组织考虑他们关于个人数据的决定可能带来的第三方成本,将负的外部性内部化,同时还能补偿个人经济损失(Brown, 2016)。

然而,另外一些研究者相信市场的力量。一些学者追随亚当·斯密的步伐,认为市场上存在一只“看不见的手”,自由放任而不是监管就能够使得市场自然达到井然有序。监管有时会产生意想不到的结果(Johnson et al, 2020b),也有一些学者挑战监管的有效性,认为监管产生了很多负面的影响。例如,阻碍市场效率、破坏创新、增加额外成本以及缺乏有效同意等。

1. 阻碍市场效率。Posner(1981)认为保护隐私会导致市场效率低下。Stigler(1980)持同样的观点,认为阻止个人信息流的监管干预措施将是再分配性的且效率低下,原因在于有关其质量的信息已在市场中被删除。根据 Taylor(2004)的观点,即使没有监管机构的干预,企业也可能出于利润最大化的目的而倾向制定隐私保护政策。

2. 破坏创新。因为隐私法规通常对个人信息的收集或使用施加限制,所以有一些学者担心隐私监管可能会影响数字市场的竞争(Gal & Aviv, 2020; Ramos & Blind, 2020),甚至破坏企业创新(Jia et al, 2019; Gal & Aviv, 2020)。例如,GDPR 把个人数据纳入详细的监管制度,并对企业施加新的责任,这将影响全球的个人数据使用。GDPR 的实施可能对新的大数据和人工智能技术的研发产生“寒蝉效应”(chilling effects)(Penney, 2021),进而危及技术进步与数字市场的创新。同样,Elkin-Koren & Gal (2019)也认为数据治理可能会产生寒蝉效应,从而扭曲数据收集和数据驱动的创新。此外,

Jia et al(2019)研究了 GDPR 对欧盟新技术风险投资的影响。结果表明,至少在短期内, GDPR 对欧盟企业有负面差异影响,损害了企业风险投资。隐私监管可能导致“投资搁浅”,而研发和创新依赖于投资的支持。

3. 增加企业成本。近期一些学者研究了隐私监管的经济影响,监管干预并非没有成本。例如, GDPR 的规模和范围会给企业带来巨大的合规成本和机会成本,已使许多企业损失数百万美元的合规成本。而且,隐私监管还增加了企业收集消费者数据的成本,使得与用户匹配的成本更高。Goldberg et al(2019)使用 DID 方法对 GDPR 在线经济影响进行了首次研究,结果表明,在 GDPR 的执行截止日期之后,欧盟用户的页面浏览量、访问量、订单和收入整体下降了约 10%。类似地, Aridor et al(2020)也证实了 GDPR 的实施降低了记录的网络流量和收入,导致 cookie 总数减少了大约 12.5%,这表明相当多的消费者决定选择退出。

4. 增加用户机会成本。一些学者认为隐私政策是写给专业人士的,由于不透明且不断变化的数据和隐私政策,消费者在了解企业的程度上处于信息不对称的地位(Economides & Lianos, 2021)。许多实证研究都强调了透明机制的局限性,其中包括隐私政策未能正确告知消费者如何使用其数据(Jensen & Potts, 2004)。然而,即使隐私政策被正确告知,消费者阅读隐私政策也需要大量机会成本(McDonald & Cranor, 2008)。并且,很少有消费者能够阅读完冗长、晦涩的隐私声明,甚至一些消费者出现隐私疲劳(Choi & Park, 2018)。

5. 缺乏有效同意。隐私政策某种程度上依赖于“通知并同意”原则,即个人应阅读隐私政策并同意或不同意服务条款。在实践中,“知情—同意”框架的实施并不容易(Baruh & Popescu, 2017)。由于在线平台通常默认采用选择加入的策略或者在用户不知情的情况下收集数据(例如剑桥分析数据丑闻),消费者行为和在线隐私保护的研究表明,“知情—同意”在很大程度上失败了,甚至演变成了一种盲目的、不知情的同意文化。

如上所述,缺乏隐私监管给国家、企业和个人都带来了相当的经济成本,甚至产生了深远的经济影响(例如全球经济金融危机)。无论是将隐私视为基本权利而依赖监管,还是将隐私作为经济商品而依赖市场,以及最近备受关注的数字事件,均表明数据立法和隐私监管是至关重要的。现在的问题是如何进行监管以促进有效和公平的竞争。综合以上分析,在数据市场中,本文建议监管关注应集中于七个方面:(1)在数据市场竞争中,将消费者视为有价值数据资源的创造者。(2)重视和评估隐私政策中“知情—同意”框架对用户的实际有效性。(3)认识到监管并不能纠正所有市场失灵,同时需要设计有效的数据市场模型。(4)关切数据法规和数据治理产生的“寒蝉效应”可能扭曲数据驱动的创新问题。(5)注意数据法规可能导致数据市场集中度意外增强,并形成垄断的问题。(6)关注以隐私为重点的法规可能会破坏公平的竞争环境的问题。(7)审核个人数据跨境流动可能的隐私风险和安全隐患问题。

六、总结与研究展望

数据已成为数字经济时代的关键生产要素,数据驱动的网络效应、规模效应和范围效应为数字经济的发展赋能。个人数据的收集和使用已成为数字经济不可或缺的一部分,伴随着以个人数据为焦点的隐私问题也日益凸显。国外隐私相关文献比较丰富,考虑到隐私的跨学科性质,本文综合法学、心理学、管理学、计算机科学和经济学等跨专业学科文献,对隐私的定义及其经济价值、隐私披露行为的理论与实证研究、隐私和消费者福利的关系、隐私和数据市场以及监管对隐私和福利的影响等多个主题进行评述,皆在全面地介绍隐私经济学的研究范围和进展。通过对现有文献的梳理总结,本文得出了以下结论:

第一,现有研究尚未形成统一的隐私定义。隐私已通过权利、商品、控制、状态和集体规范等多种方式被概念化,是一个高度依赖上下文的概念。而且,隐私定义具有明显的时代烙印,其定义随着社会发展和技术进步而不断演化。

第二,隐私不是同质产品,其经济价值呈现显著的异质性。WTA 和 WTP 仍然是衡量隐私经济价值货币化的常用手段。不同类型的个人数据的经济价值也不同,即使是同一类型的个人数据的经济价值也是因人而异。

第三,隐私行为不是衡量隐私态度的最佳指标。隐私悖论现象表现的隐私态度和隐私行为之间的不匹配是有条件的。这主要体现在隐私计算理论、社会交换理论、决策中的认知偏见和启发式、有限理性和信息不对称条件下的决策、量子同态理论、注意力以及数据外部性等多个方面。

第四,隐私和消费者福利之间的关系是非单调的。数据确权、信息不对称、价格歧视、数据二次使用、数据外部性、隐私保护与规制、数据中介策略、诱惑和成瘾性平台等都是影响两者关系的重要因素。

第五,前因—隐私关注—结果(APCO)宏观模型以及纳入行为经济学和认知心理学的变量的增强型 APCO 模型仍然是研究隐私关注问题的主流框架。

第六,隐私政策与监管是一把双刃剑。任何政策对消费者福利的影响都是双重的,数据立法和监管机构需要在消费者隐私、社会福利和企业创新之间权衡取舍。

由于隐私具有深刻的跨学科性质,所以相关内容很难面面俱到。例如,本文没有讨论隐私与健康经济学,隐私与信息安全经济学等方面的主题,也没有涉及过多的隐私增强技术(PET),包括同态加密(HE)、安全多方计算(SMPC)、差分隐私(DP)。感兴趣的读者可参阅 Acquisti et al(2016)和 Cecere et al(2017)等文献。

隐私已引起越来越多的经济学者的关注(Liu et al,2020; Garratt & Van Oordt, 2021)。隐私经济学为研究隐私问题提供了一个崭新的视角,并为数据隐私保护和隐私监管带来新的研究思路。目前,我国正处于数字化转型和数字经济快速发展时期。越来越多的经济活动由数据驱动,围绕个人数据收集和使用的隐私问题也更加突出,监管机构面临巨大挑战。针对数据安全与个人隐私问题,近期,我国的《数据安全法》《个人信息保护法》《网络安全审查办法》《互联网信息服务算法推荐管理规定》等法律法规相继颁布和实施,期望平衡数据隐私和企业创新之间的关系。然而,当前国内关于隐私经济学方面的研究处于起步阶段,未来关于隐私问题的研究应进一步关注以下几个方面:

(一)拓宽研究视角

首先,现有关于隐私问题研究的文献大多仅局限于特定领域,例如信息安全和法律等。近期,国外关于隐私问题的经济学研究比较活跃,形成了一些隐私理论和实证结果。考虑到各国的隐私政策和数据法规不尽相同,其结论的普适性尚待验证。

其次,国内在隐私经济学方面的研究刚刚起步,仍然处于摸索阶段,应借鉴国外隐私经济分析的经验研究本国的隐私问题。例如,从经济学的角度来研究《数据安全法》《个人信息保护法》等法律的实际有效性和经济后果。

最后,Hirsch (2006)指出了隐私监管和环境法之间的相似之处,Choi et al(2019)则将这种想法形式化,未来的研究可以通过环境规制的视角来研究隐私监管问题。

(二)创新研究方法

首先,如前所述,博弈论和数值模拟的方法在数据确权研究中得到了广泛应用。然而,这方面鲜有实证研究。研究过程中可能存在“过度数学化”问题,缺乏有效的经验证据,应该通过实证的研究方法对现有的隐私理论进行检验,验证理论的有效性。

其次,目前关于隐私关注问题主要通过“前因—隐私关注—结果”(APCO)宏观模型,或纳入行为经济学和认知心理学的变量的增强 APCO 模型展开研究,方法比较单一,有待创新。

(三)深化研究内容

第一,隐私本质上是一种权衡,这种权衡的结构取决于个人数据管理的技术解决方案(Wang et al, 2021)。现有信息科学的文献证明区块链技术有助于管理个人数据(Mainelli, 2017)。考虑到由于缺乏对个人数据的确权,数字经济具有“缺失市场”的特征(Economides & Lianos, 2021),未来应

该充分结合区块链等隐私增强技术(PET)进行深入研究。例如,利用区块链技术提供有效的机制授予数据主体对其个人信息使用的控制权,当未经授权的数据二次使用或隐私发生泄露时,能够对个人数据使用的第三方进行溯源和问责。

第二,关于隐私福利效应的深入探索,如个人数据的多维权衡。现有文献在研究隐私对消费者福利的影响时,通常采用单一或少数几个方面展开研究。例如针对数据确权、信息不对称、价格歧视、数据二次使用、数据外部性、隐私保护与规制、数据中介中的一个或几个因素研究隐私的福利效应,鲜有文献综合所有影响因素进行多维权衡。此外,当将这些影响因素放在一起时,彼此之间是否存在因果效应也尚不明确。另外,政策制定者还面临设计什么样的数据规则以使福利最大化的问题,这一方面仍然研究不足。

第三,现有文献主要关注隐私的福利效应,忽略了对其分配效应的研究。最近,Jann & Schottmüller(2020)研究表明,除了福利效应外,隐私还具有分配效应,而这种分配效应将如何影响隐私的实施,目前尚没有答案,也缺乏相应的系统研究。

第四,随着全球经济数字化,个人数据已成为地缘政治竞争的新前沿。一个国家的实力不仅在于其军事或贸易实力,还在于其收集、提炼和利用数据的能力(Liu, 2021)。2021年1月4日,国家网信办官网公布的《网络安全审查办法》规定,对于掌握超过100万用户个人信息的网络平台运营者赴国外上市,必须向网络安全审查办公室申报网络安全审查。可见,个人数据安全已上升到国家战略层面。随着时间的推移,个人数据的政治价值也将日益突出,目前这方面的研究有待深入。

第五,隐私经济学研究边界不清晰,相关理论也比较松散,缺乏逻辑性。考虑到隐私的跨学科性质,隐私的经济分析涉及多个学科和主题,常常让学者感到难以驾驭。尽管学者们一直为构建隐私理论、建立隐私理论和实证间的关系而努力,然而,隐私经济学的研究范围和内容仍需要进一步明确。现有的隐私理论也比较松散,彼此之间逻辑性不强,缺乏完整的研究范式。

参考文献:

- 熊巧琴 汤珂,2021:《数据要素的界权、交易和定价研究进展》,《经济学动态》第2期。
- 徐翔 厉克奥博 田晓轩,2021:《数据生产要素研究进展》,《经济学动态》第4期。
- Abowd, J. M. & I. M. Schmutte(2019), "An economic analysis of privacy protection and statistical accuracy as social choices", *American Economic Review* 109(1):171-202.
- Acemoglu, D. et al(2019), "Too much data: Prices and inefficiencies in data markets", *American Economic Journal: Microeconomics*, forthcoming.
- Acquisti, A. et al(2020), "Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age", *Journal of Consumer Psychology* 30(4):736-758.
- Acquisti, A. et al(2017), "Nudges for privacy and security: Understanding and assisting users' choices online", *ACM Computing Surveys* 50(3):1-41.
- Acquisti, A. et al(2016), "The economics of privacy", *Journal of Economic Literature* 54(2): 442-492.
- Acquisti, A. et al(2012), "The impact of relative standards on the propensity to disclose", *Journal of Marketing Research* 49(2):160-174.
- Acquisti, A. & H. R. Varian(2005), "Conditioning prices on purchase history", *Marketing Science* 24(3):367-381.
- Adjerid, I. et al(2018), "Beyond the privacy paradox: Objective versus relative risk in privacy decision making", *MIS Quarterly* 42(2):465-488.
- Akçura, M. T. & K. Srinivasan(2005), "Research note: Customer intimacy and cross-selling strategy", *Management Science* 51(6):1007-1012.
- Aleisa, N. et al(2020), "The privacy paradox applies to IoT devices too: A Saudi Arabian study", *Computers & Security* 96:101897.
- Ali, S. N. et al(2020), "Voluntary disclosure and personalized pricing", *Proceedings of the 21st ACM Conference on Economics and Computation*, pp 537-538.
- Anthony, D. et al(2017), "Toward a sociology of privacy", *Annual Review of Sociology* 43:249-269.
- Argenziano, R. & A. Bonatti(2020), "Information revelation and privacy protection", CEPR Discussion Papers, No. DP15203.

- Aridor et al(2020), "The economic consequences of data privacy regulation: Empirical evidence from GDPR", NBER Working Paper, No. w26900.
- Arpetti, J. & M. Delmastro(2021), "The privacy paradox: A challenge to decision theory?", *Journal of Industrial and Business Economics* 48(4):505—525.
- Athey, S. et al(2017), "The digital privacy paradox: Small money, small costs, small talk", NBER Working Paper, No. w23488.
- Bandara, R. et al(2021), "Construing online consumers' information privacy decisions: The impact of psychological distance", *Information & Management* 58(7):103497.
- Barnes, S. B. (2006), "A privacy paradox: Social networking in the United States", *First Monday* 11(9).
- Barth, S. & M. D. De Jong(2017), "The privacy paradox—Investigating discrepancies between expressed privacy concerns and actual online behavior: A systematic literature review"; *Telematics Inform* 34(7):1038—1058.
- Baruh, L. & M. Popescu(2017), "Big data analytics and the limits of privacy self-management", *New Media & Society* 19(4):579—596.
- Beldad, A. & M. C. Kusumadewi(2015), "Here's my location, for your information: The impact of trust, benefits, and social influence on location sharing application use among Indonesian university students", *Computers in Human Behavior* 49:102—110.
- Beresford, A. R. et al(2012), "Unwillingness to pay for privacy: A field experiment", *Economics Letters* 117(1): 25—27.
- Bergemann, D. et al(2020), "The economics of social data", Cowles Foundation Discussion Paper, No. 2203R.
- Betzing, J. H. et al(2020), "The impact of transparency on mobile privacy decision making", *Electronic Markets* 30(3):607—625.
- Bonatti, A. & G. Cisternas(2020), "Consumer scores and price discrimination", *Review of Economic Studies* 87(2): 750—791.
- Brown, I. (2016), "The economics of privacy, data protection and surveillance", in: J. M. Bauer & M. Latzer(eds), *Handbook on the Economics of the Internet*, Edward Elgar.
- Budzinski, O. et al(2021), "The economics of the German investigation of Facebook's data collection", *Market and Competition Law Review* 5(1):43—80.
- Carrascal, J. P. (2013), "Your browsing behavior for a Big Mac: Economics of personal information online", *Proceedings of the 22nd International Conference on World Wide Web*, pp. 189—200.
- Cecere, G. et al(2017), "The economics of privacy", in: M. Vernengo et al (eds), *The New Palgrave Dictionary of Economics*, Living Edition, Springer Link.
- Chen, L. et al(2021), "The data privacy paradox and digital demand", NBER Working Paper, No. w28854.
- Choi, H. et al(2018), "The role of privacy fatigue in online privacy behavior", *Computers in Human Behavior* 81: 42—51.
- Choi, J. P. et al(2019), "Privacy and personal data collection with information externalities", *Journal of Public Economics* 173:113—124.
- Ciuriak, D. (2019), "Unpacking the valuation of data in the data-driven economy", Available at SSRN: <https://ssrn.com/abstract=3379133>.
- Cloarec, J. (2020), "The personalization—Privacy paradox in the attention economy", *Technological Forecasting and Social Change* 161:120299.
- Crafts, N. (2019), "The fall in potential output due to the financial crisis: A much bigger estimate for the UK", *Comparative Economic Studies* 61(4):625—635.
- Cvrcek, D. et al(2006), "The value of location information", *Proceedings of the ACM Workshop on Privacy in the Electronic Society*, pp. 109—118.
- De Corniere, A. & G. Taylor(2020), "Data and competition: A general framework with applications to mergers, market structure, and privacy policy", CEPR Discussion Papers, No. 14446.
- Dinev, T. (2015), "Research Commentary—Informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the 'APCO' box", *Information Systems Research* 26(4):639—655.

- Dienlin, T. & S. Trepte(2015), "Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors", *European Journal of Social Psychology* 45(3):285—297.
- Dosis, A. & W. Sand-Zantman(2019), "The ownership of data", Available at SSRN: <https://ssrn.com/abstract=3420680>.
- Economides, N. & I. Lianos (2021), "Restrictions on privacy and exploitation in the digital economy: A market failure perspective", *Journal of Competition Law and Economics* forthcoming, NET Institute Working Paper.
- Eeckhout, J. & L. Veldkamp (2022), "Data and market power", CEPR Discussion Paper, No. 17272.
- Egelman, S. et al(2013), "Choice architecture and smartphone privacy: There's a price for that", in: R. Böhme(ed), *The Economics of Information Security and Privacy*, Springer.
- Elkin-Koren, N. & M. S. Gal(2019), "The chilling of governance-by-data on data markets", *University of Chicago Law Review* 86(2):403—431.
- Fainmesser, I. P. et al(2021), "Digital privacy", Available at SSRN: <https://ssrn.com/abstract=3459274>.
- Fairfield, J. A. & C. Engel(2015), "Privacy as a public good", *DUKE Law Journal* 65(3):385—457.
- Farrell, J. (2012), "Can privacy be just another good?", *Journal on Telecommunications and High Technology Law* 10(2):251—64.
- Fast, V. et al(2021), "Privacy decision-making in digital markets: Eliciting individuals' preferences for transparency", Available at SSRN: <https://ssrn.com/abstract=3987945>.
- Flaherty, D. H. (1989), *Protecting Privacy in Surveillance Societies*, University of North Carolina Press.
- Foley, S. et al(2019), "Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies?", *Review of Financial Studies* 32(5):1798—1853.
- Gal, M. S. & O. Aviv(2020), "The competitive effects of the GDPR", *Journal of Competition Law & Economics* 16(3):349—391.
- Gal-Or, E. & A. Ghose(2005), "The economic incentives for sharing security information", *Information Systems Research* 16(2):186—208.
- Garratt, R. J. & M. R. Van Oordt(2021), "Privacy as a public good: A case for electronic cash", *Journal of Political Economy* 129(7):2157—2180.
- Glasgow, G. et al(2021), "Survey response bias and the 'privacy paradox': Evidence from a discrete choice experiment", *Applied Economics Letters* 28(8):625—629.
- Goldberg, S. et al(2019), "Regulating privacy online: The early impact of the GDPR on European web traffic & e-commerce outcomes", Available at SSRN: <https://ssrn.com/abstract=3421731>.
- Gu, Y. et al(2019), "Exclusive data, price manipulation and market leadership", Available at SSRN: <https://ssrn.com/abstract=3467988>.
- Hann, I. H. et al(2007), "Overcoming online information privacy concerns: An information-processing theory approach", *Journal of Management Information Systems* 24(2):13—42.
- Hew, J. J. et al(2017), "Generating travel-related contents through mobile social tourism: Does privacy paradox persist?", *Telematics and Informatics* 34(7):914—935.
- Hirsch, D. D. (2006), "Protecting the inner environment: What privacy regulation can learn from environmental law", *Georgia Law Review* 41(1), Available at SSRN: <https://ssrn.com/abstract=1021623>.
- Hoffmann, F. et al(2020), "Persuasion through selective disclosure: Implications for marketing, campaigning, and privacy regulation", *Management Science* 66(11):4958—4979.
- Ichihashi, S. (2020a), "Online privacy and information disclosure by consumers", *American Economic Review* 110(2):569—595.
- Ichihashi, S. (2020b), "Dynamic privacy choices", *Proceedings of the 21st ACM Conference on Economics and Computation*, pp. 539—540.
- Ichihashi, S. (2021a), "Competing data intermediaries", *RAND Journal of Economics* 52(3):515—537.
- Ichihashi, S. (2021b), "The economics of data externalities", *Journal of Economic Theory* 196:105316.
- Ichihashi, S. & B. C. Kim(2021), "Addictive platforms", Available at SSRN: <https://ssrn.com/abstract=3853961>.
- Jann, O. & C. Schottmüller(2020), "An informational theory of privacy", *Economic Journal* 130(625):93—124.

- Jensen, C. & C. Potts(2004), "Privacy policies as decision-making tools: An evaluation of online privacy notices", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp 471—478.
- Jentzsch, N. (2017), "Secondary use of personal data: A welfare analysis", *European Journal of Law and Economics* 44 (1):165—192.
- Jia, J. et al(2019), "The short-run effects of GDPR on technology venture investment", NBER Working Paper, No 25248.
- Jin, G. Z. & L. Wagman(2021), "Big data at the crossroads of antitrust and consumer protection", *Information Economics and Policy* 54:100865.
- Jones, C. I. & C. Tonetti(2020), "Nonrivalry and the economics of data", *American Economic Review* 110(9): 2819—2858.
- Johnson, G. A. et al(2020a), "Consumer privacy choice in online advertising: Who opts out and at what cost to industry?", *Marketing Science* 39(1):33—51.
- Johnson, G. A. et al(2020b), "Privacy & market concentration: Intended & unintended consequences of the GDPR", Available at SSRN: <https://ssrn.com/abstract=3477686>.
- Jozani, M. et al(2020), "Privacy concerns and benefits of engagement with social media-enabled Apps: A privacy calculus perspective", *Computers in Human Behavior* 107:106260.
- Jullien, B. et al(2020), "Privacy protection, security, and consumer retention", CEPR Discussion Papers, No 15072.
- Kokolakis, S. (2017), "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon", *Computers & Security* 64:122—134.
- Krasnova, H. et al(2009), "Privacy concerns and identity in online social networks", *Identity in the Information Society* 2(1):39—63.
- Lam, W. M. W. & B. Lyons (2020), "Does data protection legislation increase the quality of internet services?", *Economics Letters* 195:109463.
- Lancieri, F. (2021), "Narrowing data protection's enforcement gap", Available at SSRN: <https://ssrn.com/abstract=3806880>.
- Laudon, K. C. (1996), "Markets and privacy", *Communications of the ACM* 39(9):92—104.
- Laufer, R. S. & M. Wolfe(1977), "Privacy as a concept and a social issue: Multidimensional developmental theory", *Journal of Social Issues* 33(3):22—42.
- Lefrere, V. et al(2020), "The impact of the GDPR on content providers", WEIS 2020: 20th Annual Workshop on the Economics of Information Security, Brussels.
- Lies, J. (2019), "Marketing intelligence and big data: Digital marketing techniques on their way to becoming social engineering techniques in marketing", *International Journal of Interactive Multimedia and Artificial Intelligence* 5(5):134—145.
- Lim, S. (2021), "Tackling privacy paradox: Protecting right to self-determination of personal information by estimating the economic value of personal information and visualizing the price", *International Journal of Internet, Broadcasting and Communication* 13(2):244—259.
- Liu, L. (2021), "The rise of data politics: Digital China and the world", *Studies in Comparative International Development* 56(1):45—67.
- Liu, Z. et al(2020), "Data privacy and temptation", Available at SSRN: <https://ssrn.com/abstract=3670488>.
- Madden, M. & L. Rainie(2015), "Americans' attitudes about privacy, security and surveillance", Pew Research Center: Internet, Science & Tech, Washington, DC, 20.
- Mainelli, M. (2017), "Blockchain could help us reclaim control of our personal data", *Harvard Business Review website*, <https://hbr.org/2017/10/smart-ledgers-can-help-us-reclaim-control-of-our-personal-data>.
- Malhotra, N. K. et al(2004), "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model", *Information Systems Research* 15(4):336—355.
- Markovich, S. & Y. Yehezkel(2021), "Data regulation: Who should control our data?", Available at SSRN: <https://ssrn.com/abstract=3801314>.
- Martens, B. (2021), "An economic perspective on data and platform market power", Available at SSRN: <https://ssrn.com/abstract=3783297>.
- Martin, S. (2020), "Market transparency and consumer search: Evidence from the German retail gasoline market",

- DICE Discussion Paper, No. 350.
- McDonald, A. & L. Cranor(2008), "The cost of reading privacy policies", *I/S: A Journal of Law and Policy for the Information Society* 4(3):543—568.
- Mothersbaugh, D. L. et al(2012), "Disclosure antecedents in an online service context: The role of sensitivity of information", *Journal of Service Research* 15(1):76—98.
- Najjar, M. S. et al(2021), "Users' affect and satisfaction in a privacy calculus context", *Online Information Review* 45(3):577—598.
- Noam, E. M. (1997), "Privacy and self-regulation: Markets for electronic privacy", in: *Privacy and Self-Regulation in the Information Age* (pp. 21—33), US Department of Commerce, National Telecommunications and Information Administration, Washington, DC.
- Hill, L. et al(2015), *Data-Driven Innovation for Growth and Well-being*, OECD Publishing.
- OECD(2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing.
- Penney, J. W. (2021), "Understanding chilling effects", Available at SSRN: <https://ssrn.com/abstract=3855619>.
- Pentina, I. et al(2016), "Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison", *Computers in Human Behavior* 65:409—419.
- Potoglou, D. et al(2015), "An integrated latent variable and choice model to explore the role of privacy concern on stated behavioural intentions in e-commerce", *Journal of Choice Modelling* 17:10—27.
- Posner, R. A(1981), "The economics of privacy", *American Economic Review* 71(2):405—409.
- Preibusch, S. (2013), "The value of privacy in web search", *IEEE Security & Privacy* 13(5):24—32.
- Ramos, E. F. & K. Blind(2020), "Data portability effects on data-driven innovation of online platforms: Analyzing Spotify", *Telecommunications Policy* 44(9):102026.
- Schaub, F. et al(2017), "Designing effective privacy notices and controls", *IEEE Internet Computing* 21(3):70—77.
- Schoch, D. S. (2020), "Mergers and acquisitions in the data economy", Available at SSRN: <https://ssrn.com/abstract=3686247>.
- Shaeffer, J. & C. N. Keever(2021), "Privacy as a collective norm", *Loyola of Los Angeles Entertainment Law Review* 41(3):253—303.
- Smith, H. J. et al(1996), "Information privacy: Measuring individuals' concerns about organizational practices", *MIS Quarterly* 20(2):167—196.
- Smith, H. J. et al(2011), "Information privacy research: An interdisciplinary review", *MIS Quarterly* 35(4):989—1015.
- Solove, D. J. (2013), "Introduction: Privacy self-management and the consent dilemma", *Harvard Law Review* 126(7):1880—1903.
- Solove, D. J. (2021), "The myth of the privacy paradox", *George Washington Law Review* 89(1):1—51.
- Solove, D. J. (2008), *Understanding Privacy*, Harvard University Press.
- Spiekermann, S. et al(2015), "The challenges of personal data markets and privacy", *Electronic Markets* 25(2):161—167.
- Stigler, G. J. (1980), "An introduction to privacy in economics and politics", *Journal of Legal Studies* 9(4):623—644.
- Taylor, C. R. (2004), "Consumer privacy and the market for customer information", *RAND Journal of Economics* 35(4):631—650.
- Trepte, S. et al(2020), "The privacy calculus contextualized: The influence of affordances", *Computers in Human Behavior* 104:106115.
- Urbonavicius, S. et al(2021), "From social networking to willingness to disclose personal data when shopping online: Modelling in the context of social exchange theory", *Journal of Business Research* 136:76—85.
- Varian, H. R. (1996), "Economic aspects of personal privacy", in: W. H. Lehr et al(eds), *Internet Policy and Economics*, Springer.
- Wang, C. A. et al(2021), "Managing privacy in the digital economy", *Fundamental Research* 1(5):543—551.
- Warren, S. D. & L. D. Brandeis(1890), "The right to privacy", *Harvard Law Review* 4(5):193—220.
- Westin, A. F. (1968), "Privacy and freedom", *Washington and Lee Law Review* 25(1):166—170.

- Westin, A. F. (2003), "Social and political dimensions of privacy", *Journal of Social Issues* 59(2):431—453.
- Wottrich, V. M. (2018), "The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns", *Decision Support Systems* 106:44—52.
- Xu, H. & S. Gupta(2009), "The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services", *Electronic Markets* 19(2):137—149.
- Yu, J. et al(2015), "Role of affect in self-disclosure on social network websites: A test of two competing models", *Journal of Management Information Systems* 32(2):239—277.
- Zhu, Y. Q. & K. Kanjanamekanant(2021), "No trespassing: Exploring privacy boundaries in personalized advertisement and its effects on ad attitude and purchase intentions on social media", *Information & Management* 58(2):103314.
- Zuboff, S. (2019), *The Age of Surveillance Capitalism: The Fight For A Human Future at the New Frontier of Power*, New York: PublicAffairs.

Research Progress on Economics of Privacy

JIA Chuanchang ZHU Jianming GAO Sheng

(Central University of Finance and Economics, Beijing, China)

Abstract: The continuous development of the digitalization of the economy and the advancement of data processing technology have aroused economists' great interest in the role of personal information in production. The economics of privacy is an emerging research field belonging to information economics. It focuses on the allocation of a special type of resource (personal information) and is an interdisciplinary subject that uses the basic principles and methods of economics to analyze and explain privacy phenomena or problems. This paper firstly introduces the concept of privacy and its economic value, and emphasizes the dynamic evolution characteristics of privacy concept and the heterogeneity of privacy economic value. Afterwards, this paper explores the decision-making process for sharing personal data, further analyzes what factors contribute to the disclosure of personal information, and the assumptions under which the privacy paradox exists. Then, this paper discusses the welfare effects of privacy on consumers from the aspects of data right confirmation, information asymmetry, price discrimination, secondary use of data, data externality, privacy protection and regulation. It analyzes the mechanism by which privacy leads to the failure of the data market, summarizes the economic impact of privacy regulation, and reiterates the privacy issues that regulation should pay attention to. Finally, this paper discusses some deficiencies in privacy economics research and points out directions for future research.

Keywords: Economics of Privacy; Personal Data; Privacy Paradox; Data Market; Consumer Welfare

(责任编辑:刘洪愧)

(校对:李仁贵)