

· 研究论文 ·

隐私悖论研究述评及未来展望

罗映宇¹ 韦志颖² 孙锐²

(1. 湖南大学工商管理学院,长沙,41000; 2. 华侨大学工商管理学院,泉州,362000)

[摘要] 近年来,隐私悖论已成为管理学、情报学等领域的热点话题,但是目前学术界仍缺乏系统性的认识和指导,严重制约了隐私悖论研究的发展。本研究通过回顾和梳理近年来的研究成果,从隐私计算、有限理性、社会理论、解释水平和量子力学五个方面对隐私悖论的研究成果进行归纳和探讨,提出当前研究存在争议的三大原因:定义模糊、方法失位、群体受限,并对未来隐私悖论的研究方向进行展望,以期为进一步的研究提供参考。

[关键词] 隐私悖论 隐私关注 隐私态度 隐私计算

[中图分类号] G201;C912.3 [文献标识码] A [文章编号] 2095-2171(2020)05-0066-10

DOI: 10. 13365/j. jirm. 2020. 05. 066

Review of Privacy Paradox Research and Future Prospects

Luo Yingyu¹ Wei Zhiying² Sun Rui²

(1. Business School of Hunan University, Changsha, 410000; 2. Huaqiao University School of Business Administration, Quanzhou, 362000)

[Abstract] In recent years, privacy paradox has become a hot topic in management, information science and other fields, but the current academic community still lacks systematic understanding and guidance, which seriously restricts the development of privacy research. By reviewing and combing the research results in recent years, this paper summarizes and discusses the research results of privacy paradox from five aspects: privacy calculus, bounded rationality, social theory, construct level and quantum theory, and proposes three major controversies in current research: definition ambiguity, method misplacement, group restriction. It prospects for the future research direction of privacy paradox, in order to provide reference for further research.

[Keywords] Privacy paradox; Privacy concern; Privacy attitude; Privacy calculation;

1 引言

2018年,剑桥分析事件使 Facebook 和美国遭受巨大的隐私信用危机。Facebook 首席

执行官马克·扎克伯格在美国国会中承认:“我们有责任保护用户隐私,如果做不到,就不该继续为用户服务”^①。为什么 Facebook 声称

[基金项目] 本文系华侨大学研究生科研创新能力培育计划项目(17013121006)。

[作者简介] 罗映宇,博士研究生,研究方向为神经营销学;韦志颖,硕士研究生,研究方向为神经营销学;孙锐(通讯作者),教授,博士生导师,研究方向为知识管理,神经营销学,Email:15880918120@163.com。

① 引自《美国国会传唤扎克伯格:就5000万用户数据泄露案作证》[EB/OL].[2019-03-20].http://sohu.com/a/226206293_260616.

本文引用格式:罗映宇,韦志颖,孙锐.隐私悖论研究述评及未来展望[J].信息资源管理学报,2020,10(5):66-75.

要保护用户隐私? 隐私数据有什么用? 事实上, 现有的网络公司已经意识到, 在与对手的竞争中, 没有大数据的支撑无疑是“盲人瞎马”“危如累卵”, 因此, 以精准推荐为核心的个性化推荐系统根植于网络公司发展的地基之上^[1]。但是这项以精准为核心的技术面临一个严峻的挑战——“隐私悖论 (Privacy Paradox)”, 即用户普遍担心自己的隐私信息遭受泄露, 同时又愿意披露自己的隐私^[2]。这种奇特的现象使大数据的发展面临两难, 西方学界从 2006 年起对隐私悖论进行了大量研究, 特别是社交网络 (SNS) 下的隐私悖论^[3], 但遗憾的是, 目前仍缺乏一个系统性的框架去理解和把握该研究, 而且不少学者对隐私悖论还持有浅显或错误的观点^[4], 对这一现象背后的理论概念尚未厘清^[5], 这些都严重制约了隐私悖论研究的进一步发展。

以“privacy paradox”和“隐私悖论”为主题词, 分别对 2010—2019 年间 Web of Science 和 CSSCI 数据库中的文献进行检索, 得到外文文献 74 篇、中文文献 14 篇。通过对这些文章及早期经典文章进行梳理后发现存在三个问题, 一是缺乏系统性梳理, 目前隐私悖论的研究已初具规模, 但是研究较为零散, 理论单一, 尚未对隐私悖论的研究形成系统性的认识^[6-7]; 二是尚存一定的研究争议, 由于定义模糊、使用研究方法不恰当和研究受限的原因, 目前学界对隐私悖论的研究结果存在不一致的看法^[8-9]; 三是研究展望的局限性^[10], 现有研究虽然从不同方面提出未来的研究方向, 但仍然存在局限性, 未提出明确性和指导性的建议, 对研究的把握不足。为梳理隐私悖论的研究脉络, 剖析现有的研究问题, 下文将从隐私悖论的研究成因、理论整合、争议和研究展望进行论述。

2 隐私悖论的成因

隐私悖论早期的研究大约在 1998 年到 2007 年之间。这一时期的研究主要是解释隐私态度和隐私行为不一致的现象, 尚未提出“隐私悖论”这一概念, 可分为三个阶段: 隐私悖论现象的发现、隐私悖论理论解释的引入、隐私悖论术语及研究体系的建立。

隐私悖论的研究最初发表于医学领域。1998 年, 分析人员做了一项实验, 他们要求患者允许其使用或发表病患临床材料, 但是患者不希望“隐私”信息公之于众, 因此受到患者的强烈抵制。有趣的是, 当研究者给出一份权威的解释信息后, 患者们的态度发生了转变。研究者认为合理的解释或信任能够使个体做出看起来不那么合理的行为, 例如暴露隐私^[11]。随后, 研究逐渐延伸到消费行为领域, 研究人员对使用优惠卡的消费者进行访谈后发现, 尽管消费者对于他们的隐私信息被收集表现出很强的担忧, 但仍然会为了能够使用优惠卡交换个人信息^[12]。在一项网络购物研究中, 研究人员先让消费者自述对隐私的态度, 之后通过一些操作来观察消费者对于隐私信息的处理, 最终发现, 消费者自述时对隐私信息表现出强烈的关注, 但是在收益的情况下, 消费者依然会披露自己的隐私信息, 即使这些信息是高度私密的^[13]。早期的研究虽注意到人们在隐私行为中的反常现象, 但是并未对其进行深入的研究。

在隐私态度与隐私行为不一致现象被发现后不久, 研究者开始尝试引入理性行为理论对这一现象进行解释。Acquisti 等^[14]将 Gilovich 等^[15]在有限理性等方面的发现融入自己的研究, 建立了即时满足行为经济模型, 该模型认为, 相较于未来的风险, 人们更注意目前的收益, 因此, 人们会因为对未来收益的不确定而不会采取一个严格的隐私保护。这一理论的引入, 在一定程度上对“隐私悖论”现象给予了解释。2005 年, Acquisti 等又引入不完全信息、有限理性和心理偏见理论进行了一项实证研究, 研究结果丰富了该项研究的视角。同时, 他们希望对这种现象提出一个新的定义^[16], 此前, 学界对“隐私悖论”仍然使用“隐私态度与行为分歧”这一概念。

在理性理论被引入不久后, “隐私悖论”的研究体系开始建立。2006 年, Barnes 在社交网络研究中首次使用了“隐私悖论”这一术语^[17]。随后, Norberg 等通过对实际市场中消费者的隐私行为进行观察后发现, 人们在保护自身隐私数据方面并不挑剔, 甚至常常主动泄露隐

私^[18]。在此之前,较少研究关注个体隐私保护意愿和实际购买行为之间的差异,Norberg等的研究为隐私悖论研究打破调查方法的限制作出了突出贡献,同时,他提出人们对风险的感知和对目标的信任有助于解释为什么会出现隐私悖论。此外,Norberg等还对隐私政策进行了初步讨论,目的是探讨在隐私侵蚀不可避免的情况下,人们将如何应对和作出反应。通过上述研究,Norberg等建立了隐私悖论的研究体系。

3 隐私悖论研究理论整合

通过系统梳理隐私悖论的研究现状,将隐私悖论理论研究划分为五个群类(表1):①隐私计算理论,这是目前使用最广泛的理论,该群类可细分为基于理性的隐私计算和基于有偏的隐私计算;②有限理性,分为信息不对称、能力和知识有限;③社会理论;④解释水平理论;⑤量子力学理论。

3.1 隐私计算理论

隐私计算模型是当下隐私研究中最常用的模型。一些研究认为,个体的隐私计算过程解释了隐私关注与隐私行为之间出现的矛盾行为,即用户在有意识的权衡隐私披露的预期损失和潜在收益后作出隐私披露决策^[19-20]。但是决策行为往往受到认知偏差和启发式的影响,这使得个体实际上无法对隐私披露行为的收益和损失作出正确的估计,常常重视利益而忽视伴随的风险^[21]。

3.1.1 基于理性的隐私计算

基于“理性人”假设,经济活动的参与者都试图用最小的代价获取最大的利益,因此,个体会在进行风险-收益计算后采取行动^[22]。在隐私计算中,感知收益指的是经济效益、个性化、方便性、社会效益^[23]、社会资本^[24]以及娱乐需求、社会关系需要、身份建设需要^[25],侵犯隐私^[26]、身份盗取^[27]、网络欺凌^[28]则代表感知风险,感知收益往往被认为能抵消感知风险的负面影响。一项在社交网络中进行的研究表明,当用户的感知收益大于潜在风险时,用户往往会选择披露个人隐私,这种观点较好地解释了隐私悖论现象。也有学者认为,隐私行为因个体特质而异,例如,Penina等的研究发现,外向性和随和性个体更能感知到收

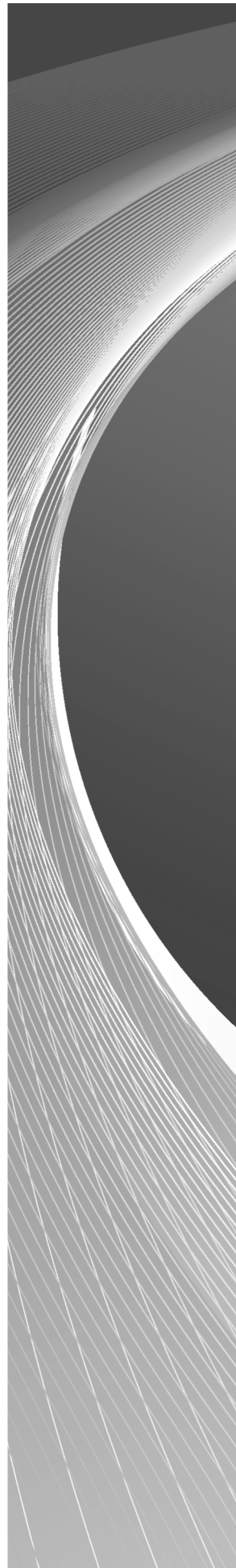
益^[29],这将导致更多的隐私分享活动。这项研究同时提出:因为预先存在的态度(例如隐私问题)可能会被情境因素(如福利协会)完全推翻,因此隐私计算必须考虑情境因素^[30]。

3.1.2 基于有偏的隐私计算-认知偏差(Cognitive Bias)

在某些特定情况下的特定思考和行为倾向会导致理性判断出现系统性偏差,个体只能进行有偏差的风险-收益评估^[31]。这些偏差往往无法改变或被意识到,但是对最终的决策产生着重大的影响^[16]。消费者行为的研究也表明,决策过程受到各种认知偏差和启发式的影响^[32]。为探析认知偏差对隐私计算的影响,研究从启发式、即时满足、乐观偏见、控制错觉四个方面阐释。

(1)启发式(Heuristic)。启发式是一个经验法则,是一条人们基于自己的经验、知识和直觉作出快速判断的心理捷径^[33]。依据启发类型的不同,可分为可获得性启发式、情感启发式、利益启发式和模糊边界启发式。可获得性启发式表明人们认为那些易于想起的事件更有价值,因而人们会高估社交网络中常见事件的价值^[34];情感启发式指的是人们基于他们的情感印象进行判断,包括两项准则:一是个体倾向于低估他们喜欢事物的风险而高估他们厌恶事物的风险,二是个体倾向于高估他们喜欢事物的收益而低估厌恶事物的收益^[35];模糊边界启发式和利益启发式在功能上有显著差异,Sunder等的研究表明,模糊边界启发式不太可能披露个人信息,而利益启发式则倾向于披露更多关于个人的信息^[36]。

(2)即时满足(Immediate Gratification)。即时满足风险指的是人们倾向于立即得到满足(如快速下载手机应用获得其服务)而忽略未来的风险^[33]。研究者认为,个人倾向于低估未来高风险事件(如身份盗窃)的发生概率,从而满足自己对当前利益的需要^[37]。在隐私计算中,个体通常认为隐私披露获得的利益高于风险造成的损失,这种即时满足破坏了个体对隐私披露的担忧,导致个体不采用或较少采取隐私保护措施,增加了将来遇到隐私侵犯的可能性^[23]。



(3) 乐观偏见 (Optimistic Bias)。乐观偏见指出,个人往往会低估自己受到隐私侵犯的风险,同时高估他人遭遇风险的可能性^[33]。研究认为乐观偏见会降低个体风险感知的程度,这将导致个体较少关注甚至忽视隐私披露行为造成的风险,诱发人们披露更多的隐私;同时还会使人们低估风险事件发生的概率并高估信息披露带来的好处,从而诱发人们披露更多的隐私^[38]。

(4) 控制错觉 (Illusion of Control)。控制错觉指的是高估自己能够控制某种东西的倾向^[39]。研究指出,用户在感到自己有对信息的控制权时,更愿意公布自己的信息,甚至是敏感性信息^[40-41]。但是,如果第三方介入隐私信息活动,用户便会感到自己失去了对信息的控制,从而不愿意披露个人信息^[42]。因此,实践界和学界尝试引入控制权这一概念,例如给予用户在社交网络上设置隐私的权力(虽然实际上并没有效果),实践证明该项措施有效地缓解了用户的隐私抵触行为^[43]。

3.2 有限理性 (Bounded Rationality)

有限理论认为,由于个体在进行决策时既无法获取全部信息,又不具备充足的知识与能力,因此,在进行隐私披露行为时并非完全理性^[33]。基于现有的研究,可将有限理性分为信息不对称、能力与知识有限两方面。

(1) 信息不对称 (Information Asymmetry)。个体在作出信息披露决策时,博弈双方所获取的信息并不是完全相同的^[39]。随着大数据的使用和个人数据市场的出现,信息不对称现象更加普遍^[44]。研究认为用户不可能了解所有隐私的详尽信息,包括隐私信息价值、收集路径、收集状态等^[35],也就难以对隐私披露的后果进行计算^[38]。因此,研究者认为基于不完全信息作出的决策,由于风险和收益无法得到适当的评估,所以输出的是有限理性的结果^[45]。

(2) 能力与知识有限。在用户能够获得全部信息的前提下,用户缺乏比较风险和收益的计算能力和知识也是隐私悖论现象产生的重要原因^[46]。以往的研究发现,多数用户因缺乏技术(例如删除 cookie、加密电子邮件等)和法律方面的隐私保护知识^[47],也就难以对潜在的隐

私威胁进行评估和采取隐私保护行为。此外,隐私披露在互联网活动中尤为常见,用户会认为他们没有有效的方法来管理他们在互联网上的个人信息,这种对隐私问题的厌倦感被称为隐私疲倦 (Privacy fatigue)^[48]。在这种感觉中,用户不愿意花费大量的精力来管理他们的隐私信息,也不会采取隐私保护行为^[49]。

3.3 社会理论 (Social Theory)

人具有社会性,用户分享自己的隐私是为了获得更多社交机会,符合使用社交网络的基本动机^[50-51]。同时,个体的存在和身份都源自集体,同一集体的人们有着相似的观点和经验,这些观点和经验对于其成员有着近乎强制性的影响力^[52]。

大多数人在接受或拒绝使用应用程序、社交网络或电子邮件加密时并非是完全自主的,人们所处社会环境影响着个体的行为^[53]。例如,在集体主义文化中,集体意识会促使人们遵守默认规则(比如隐私披露)^[54-55]。在个体主义文化中同样存在这种倾向,一项在美国的研究表明,孩子对于隐私分享的态度常与父母相似^[56]。同时,社交网络已渗入人们的社会生活中,即使人们担心隐私安全,但为了维持正常的社交生活,也会选择披露个人隐私^[52]。另外,因为社交网络中一些人已经自我披露了一些信息,基于互惠的理念和社会公平的压力,那些没有披露个人信息的人也被要求披露信息^[38],甚至不分享个人信息会被认为是一种耻辱^[57]。研究社会理论的学者认为,个人的实际行为会受到社会关系、社会规范、社会角色、社会制度等多种社会因素的影响,无法完全自由作出决策,这也直接影响了个体隐私活动^[2,14]。

3.4 解释水平理论 (Construal Level Theory)

解释水平理论是近 20 年发展起来的纯认知理论,它建立在心理距离的四个维度上(时间距离、空间距离、社会距离、可能性)探讨心理距离对解释水平及个体行为的影响^[58]。该理论认为心理距离通过影响解释水平进而影响个体对未来事件的意向或行为。对于那些发生在时间距离远、空间位置间隔远、常在他人身上发生或发生在自己身上概率较低的事件,在心理上人们更倾向用高解释水平来表

征,即会用更抽象的、本质的方式理解这些事件。反之,对于近心理距离的事物或者时间,人们倾向用低解释水平表征,并对空间距离近、接近自我的事件产生重要影响。

在实际中发现,用户的隐私关注与隐私行为之间不存在相关关系,也就是常说的隐私悖论^[2,14]。解释水平理论对此的解释是,大数据环境下用户对隐私的认知尚未明确,隐私处于抽象、背景化的高解释水平,在此背景下,用户的实际意图和行为很难预测^[59-60]。正因此,现有学者多从具体认知角度入手对隐私悖论进行解释^[61],比如隐私计算理论衡量收益和损失^[62],认知偏差理论考虑个体的乐观程度、自信等因素^[63],社会资本理论将隐私分享行为作为一种个体的社会关系资本^[64],也有学者将解释水平理论和计划行为理论整合用于解

释个体长远的披露意愿和行为^[65]。

3.5 量子理论(Quantum Theory)

Flender 和 Muller 基于量子理论对隐私悖论提出一种新的解释。他们认为个体的隐私披露行为和量子实验的测量具有相同的效果,即决策结果在决策完成时才能确定^[66]。例如在隐私行为中,个体的隐私披露行为不受其隐私态度的影响,呈现出不确定性,也就是常说的隐私悖论,而这个不确定性将随着个体作出决策后消失,并且这两个过程是不可互换的^[38,67]。量子理论从物理学角度对隐私悖论进行阐释,一定程度上丰富了研究的理论视角且具有新颖性,但是该理论存在着“过于简化”以及“难以预测”的弊端,在实际隐私行为中仍难以运用。

表 1 隐私悖论理论群体、代表作者及观点

理论群体	代表作者	代表观点归纳
隐私计算	TDinev & P Hart; H Krasnova; H Li 等 ^[81,19]	经济活动的参与者都试图用最小的代价获取最大的利益,因此个体会在进行风险-收益计算后采取行动。
有限理性	Waldman A E ^[39] ; Choi H ^[49] ; Christofides E ^[43] 等	由于信息的不对称性和个体认知能力和知识的缺失,人的理性是有限的。因此个体在进行决策时既无法获取全部信息,又不具备充足的知识与能力,在进行隐私披露行为时并非是完全理性的。
社会理论	Agi & Jullien; Blank, Bolsover, & Dubois 等 ^[50,52]	人具有社会性,用户分享自己的隐私是为了获得更多社交机会,符合使用社交网络的基本动机。
解释水平理论	Y Trope; H Li; Bandar 等 ^[19,6]	人们对事件的解释会随着对事件的心理距离知觉的变化而发生变化,进而影响人们的行为。
量子力学理论	Flender & Muller ^[38]	决策结果只有作出决策那一刻才知道。

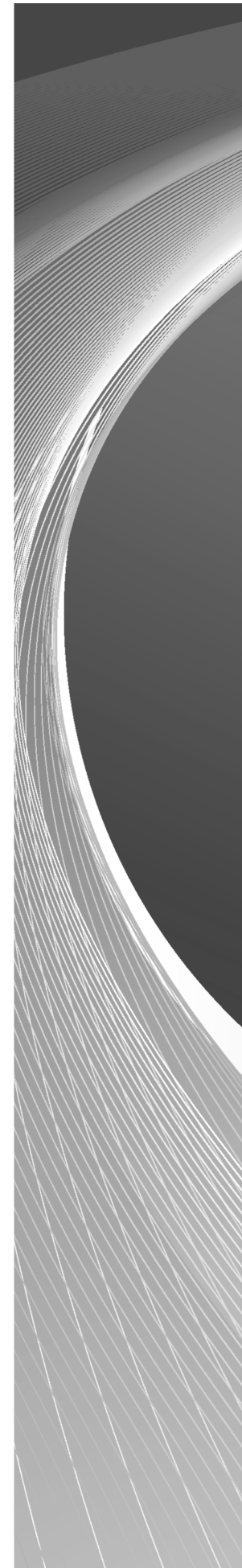
4 隐私悖论的研究争议

隐私悖论这一现象是近年来新兴的议题。大部分学者认为隐私关注不会影响用户隐私披露行为^[53],即尽管用户十分关注隐私安全问题,但他们还是积极地分享个人信息。这是因为他们在进行隐私披露时,会综合考虑隐私披露的风险与预期收益,当预期收益大于风险时,他们更倾向于选择披露隐私^[21],这在一定程度上解释了隐私悖论现象。然而,另一部分学者认为隐私态度和隐私保护行为之间并不存在二分法,而是二者具有一致性^[5]和正相关关系^[55]。针对隐私悖论目前存在的种种争议,通过对当前学界有关隐私悖论的研究进行系统的分析和归纳,梳理出了隐私悖论广存争议的三大原因,即定义模糊、方法失位、群体

受限。

4.1 定义模糊

隐私悖论的定义繁多,主要包括:①隐私关注(Privacy Concern)和隐私态度(Privacy Attitude)的不一致;②隐私关注/隐私态度和隐私披露意愿(Privacy Disclosure Intention)/行为(Privacy Disclosure Behavior)的不一致。目前应用较为广泛的定义是指隐私态度与隐私行为之间的不一致性。实际研究中,隐私关注和隐私态度都是对具体隐私行为的评价,只是侧重的维度有所区别。隐私披露意愿与隐私行为之间也有质的区别,但隐私意愿并不一定引致隐私行为^[4]。现有研究中,多数学者将隐私关注与隐私态度划等号,隐私意愿与隐私行为划等号,这是当前研究缺乏统一定义的原



因^[2,14]。

4.2 方法失位

隐私悖论的研究主要的是采用定量研究方法。定量研究中以调查法居多,并且许多是在线调查。以往的研究认为,调查法可能适用于探索信念和态度,却不适合实际行为,这就导致对隐私披露行为的测量并不可靠^[67]。同时,行为通常被评估为一个二分法的答案(例如通过询问某人是否有公开的 Facebook 个人资料),而态度则用一个度量尺度(例如基于 likert 量表)来衡量,这会导致统计上的不匹配。此外,调查法在探索不规则或不频繁的行为(例如隐私披露行为)时并不可靠^[67],例如,学者通过对比 Google+ 用户的调查反应和实际行为发现,实际行为比调查反应更为强烈,并且对于那些不规律和不常见的行为(比如隐私设置),报告反应的准确性更低^[68]。综上,在隐私悖论研究中研究方法失位是导致目前研究结论混乱的一大原因。

4.3 群体受限

目前研究中对隐私悖论研究人群的涵盖面较广。总体来看,研究对象以网络使用较为频繁的年轻人(18—35岁)居多。但是这也面临着一些问题,例如一项社交网络研究发现,年轻人有着较低的个人隐私关注和更大隐私保护行为,这与之前认为年轻人更容易泄露隐私的结论有所不同^[69]。Blank 的研究进一步佐证了这一观点,他发现隐私关注和隐私悖论之间存在着正相关关系,年龄和隐私行为呈现负相关关系,年轻人更愿意采取行动保护隐私^[52]。有学者提出,年轻的用户更喜欢采取策略去保护自己的隐私,例如提供错误信息、限制好友请求并删除标记与照片、更改个人隐私设置等方法^[70]。在实际研究中,尽管以年轻人甚至是学生为研究对象操作性较强、消耗研究资源较少,但是在隐私行为研究中,以年轻人为研究对象极易造成研究的结果前后矛盾,损害研究的普遍性和有效性^[71]。

5 研究结论和展望

5.1 研究结论

大数据技术的蓬勃发展使得企业能够实现

对用户隐私信息更深层次的挖掘和利用。以往研究发现,尽管用户都声称高度关注隐私,但是他们仍然选择继续披露自己的隐私信息以获取在线平台便利的服务^[2,14]。早期国外学者对隐私悖论的起因进行了一定程度的探索,初步引入了隐私悖论术语、建立起隐私悖论的研究体系^[17-18]。近 10 年来,已有研究从不同的理论角度对隐私悖论现象进行了研究,主要分为隐私计算理论、有限理性、社会理论、解释水平理论、量子力学理论这五类理论群体,同时仍存在一定的争议,定义模糊、方法失位和群体局限则是学者们对隐私悖论现象是否存在、结果是否一致持有不同意见的主要原因。

5.2 展望

隐私悖论是当前信息环境下讨论的热点话题。百度 CEO 李彦宏曾表示:“中国人不注重隐私,如果可以,他们更愿意用隐私换取便利。”^①这句话引发了学者对数字化时代公民隐私意识的思考。人们的隐私行为是否难以预测,或者说是否存在隐私关注和隐私行为的悖论,国内外对比的研究虽取得了一定的成果,但是隐私悖论的研究仍处于探索阶段,对隐私悖论的研究范围、解释深度、研究规范等仍未有系统的研究,为进一步探索隐私悖论的发展空间,本研究认为可从以下三个方面进行深入探讨。

(1) 电子商务下的隐私悖论。现有的研究主要是研究社交网络(SNS)下的隐私悖论,对电子商务下的用户隐私行为研究较少,但是,现有的研究其实已经对这方面有了初步的探讨^[72]。比如推荐解释,即告诉用户如何使用信息。推荐解释被证实可以提升信任^[73]、满意度^[74]、增强信息说服力、减少用户的决策损耗^[75],促进用户对推荐信息的接纳^[76],培养用户对该产品领域的了解^[77]。后期研究发现,基于用户个人隐私的推荐解释一定程度上诱发了用户的抵触情绪,学者进而提出合理化解解释,即告诉用户为什么使用这些信息^[78],这项举措被证实是一个有效的说服方式^[79]。这些研究都意识到透明度、信任、控制感等因素对用户实际接受行为的重要影响,但遗憾的是他

① 引自《称中国人不重视隐私,李彦宏再次把百度推上了风口浪尖》[EB/OL].[2019-03-20]. http://sohu.com/a/226577027_393779.

们并未对用户隐私关注和隐私态度进行讨论。

(2) 神经科学研究。隐私计算理论是目前使用最广泛的理论,该理论认为用户披露信息的行为是经过一系列计算后的结果,当收益大于损失后用户便会采取披露行为。但是,该理论的可靠性受到了一定的质疑,一是因为隐私计算模式就像一个“黑箱子”,没人知道里面发生了什么^[80-81];二是计算过程是假设性的,有学者认为分享信息是即时性的,用户并没有计算得失的可能^[82]。采用现有的研究方法(例如调查法)难以剖析用户隐私行为背后的原因,这也限制了隐私悖论研究进一步的发展。

神经科学的引入则有效地解决了该项问题。特别是关联学科神经管理学(Neural marketing)和神经营销学(Neural Marketing)的发展,为这方面的研究打下了基础。神经科学通过探索用户决策过程中脑区的激活,用即时、灵敏、客观指标分析特定的心理现象^[83]。例如,孙锐等的研究发现,形成自我知觉的个体隐私态度和隐私行为更趋近一致;相应地,形成自我知觉的个体大脑前额叶和顶叶诱发的认知

冲突更低,这项研究为揭示隐私悖论的认知机制提供了新的视角^①。需要注意的是,尽管神经科学实验能揭示用户决策过程中的心理反应,但是该研究方法对实验室具有极高的要求,需要控制颜色、声音、电磁等因素的影响^[83]。因此,营造一个真实、合理的实验情境是该研究领域亟待解决的问题。

(3) 跨文化研究。2018年5月25日,欧洲里程碑式的个人隐私保护法案《通用数据保护条例》正式生效,英国《独立报》称之为“互联网诞生以来最大的变革”^[84]。这项史上最严格的隐私保护法说明欧洲在数据保护上走在前列。而在中国,隐私问题正激起广泛讨论,中国人是不是真的不如外国人注重隐私,中国与国外的隐私悖论是否有显著的差异,这都是值得思考的问题。客观来说,众多跨文化的研究证实了同一问题在中外的差异,从而促使我们关注隐私悖论在国内外情境下的异同,特别是将同样的隐私问题引入中国是否适用或者相应的理论是否可以完全解释的问题。

参考文献

- [1] Machanavajjhala A, Korolova A, Sarma A D. Personalized social recommendations: Accurate or private[J]. Proceedings of the VLDB Endowment, 2011, 4(7): 440-450.
- [2] Kokolakis S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon [J]. Computers & security, 2017, 64: 122-134.
- [3] 谢兴政,蔡念中,黄志铭,等. 社交媒体用户隐私悖论行为影响因素初探 [J]. 图书情报工作, 2018, 62(18): 55-63.
- [4] Lee N, Kwon O. A privacy-aware feature selection method for solving the personalization-privacy paradox in mobile wellness healthcare services [J]. Expert Systems with Applications, 2015, 42(5): 2764-2771.
- [5] Heravi A, Mubarak S, Choo K-K R. Information privacy in online social networks: Uses and gratification perspective [J]. Computers in Human Behavior, 2018, 84: 441-459.
- [6] Bandara R, Fernando M, Akter S. The privacy paradox in the data-driven marketplace: The role of knowledge deficiency and psychological distance[J]. Procedia Computer Science, 2017, 121: 562-567.
- [7] Park S Y, Morton C R. The role of regulatory focus, social distance, and involvement in anti-high-risk drinking advertising: A construal-level theory perspective[J]. Journal of Advertising, 2015, 44(4): 338-348.
- [8] Baek Y M. Solving the privacy paradox: A counter-argument experimental approach [J]. Computers in Human Behavior, 2014, 38(3): 33-42.
- [9] 刘婷,邓胜利. 国外隐私悖论研究综述 [J]. 信息资源管理学报, 2018, 8(2): 104-112.
- [10] 张玥,朱庆华. 国外信息隐私研究述评 [J]. 图书情报工作, 2014, 58(13): 140-148.
- [11] Furlong A. Should we or shouldn't we? Some aspects of the confidentiality of clinical reporting and dossier access [J]. The International Journal of Psycho-analysis, 1998, 79: 727-739.
- [12] Smith A, Sparks L. Making tracks: Loyalty cards as consumer surveillance[J]. ACR European Advances, 2003, 6:

① 孙锐,罗映宇. 自我知觉理论视角下消费者隐私悖论行为研究:ERPs的证据. 该研究已被《南开管理评论》录用,目前还未刊出

- 368-373.
- [13] Brownchidsey R, Boscardin M L, Sireci S G. Computer attitudes and opinions of students with and without learning disabilities[J]. *Journal of Educational Computing Research*, 2001, 24(2): 183-204.
- [14] Acquisti A, Grossklags J. Privacy attitudes and privacy behavior[M]//*Economics of Information Security*. Springer, Boston, MA, 2004: 165-178.
- [15] Gilovich T. Heuristics and biases[M]. Cambridge: Cambridge University Press, 2002.
- [16] Acquisti A, Grossklags J. Privacy and rationality in individual decision making [J]. *IEEE Security & Privacy*, 2005, 3(1): 26-33.
- [17] Barnes S B. A privacy paradox: Social networking in the United States[J]. *First Monday*, 2006, 11(9): .
- [18] Norberg P A, Horne D R, Horne D A. Privacy paradox: Personal information disclosure intentions versus behaviors [J]. *Journal of Consumer Affairs*, 2007, 41(1): 100-126.
- [19] Krasnova H, Veltri N F. Privacy calculus on social networking sites: Explorative evidence from Germany and USA [C]//2010 43rd Hawaii International Conference on System Sciences. IEEE, 2010: 1-10.
- [20] Debatin B, Lovejoy J P, Horn A K, et al. Facebook and online privacy: Attitudes, behaviors, and unintended consequences[J]. *Journal of Computer-Mediated Communication*, 2009, 15(1): 83-108.
- [21] Lee H, Park H, Kim J. Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk[J]. *International Journal of Human-Computer Studies*, 2013, 71(9): 862-877.
- [22] Karwatzki S, Dytynko O, Trenz M, et al. Beyond the personalization-privacy paradox: Privacy valuation, transparency features, and service personalization[J]. *Journal of Management Information Systems* 34.2 (2017) : 369-400.
- [23] Wilson D, Valacich J S. Unpacking the privacy paradox: Irrational decision-making within the privacy calculus[J]. *Telematics and Informatics*, 2019,41: 114-125.
- [24] Stutzman F, Capra R, Thompson J. Factors mediating disclosure in social network sites[J]. *Computers in Human Behavior*, 2011, 27(1): 590-598.
- [25] Debatin B, Lovejoy J P, Horn A K, et al. Facebook and online privacy: Attitudes, behaviors, and unintended consequences [J]. *Journal of Computer-Mediated Communication*, 2009, 15(1), 83-108.
- [26] Eastin M S, Brinson N H, Doorey A, et al. Living in a big data world: Predicting mobile commerce activity through privacy concerns[J]. *Computers in Human Behavior*, 2016, 58: 214-220.
- [27] Martin K E. Ethical issues in the big data industry[J]. *MIS Quarterly Executive*, 2015, 14: 2.
- [28] Markus M L. New games, new rules, new scoreboards: The potential consequences of big data [J]. *Journal of Information Technology*, 2015, 30(1): 58-59.
- [29] Pentina I, Zhang L, Bata H, et al. Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison[J]. *Computers in Human Behavior*, 2016, 65: 409-419.
- [30] Kehr F, Wentzel D, Kowatsch T. Privacy paradox revised: Pre-existing attitudes, psychological ownership, and actual disclosure[J]. *Association for Information Systems*, 2014, 12: 1-15.
- [31] Knijnenburg B P, Kobsa A, Jin H. Dimensionality of information disclosure behavior[J]. *International Journal of Human-Computer Studies*, 2013, 71(12): 1144-1162.
- [32] Wattanacharoensil W, La-ornual D. A systematic review of cognitive biases in tourist decisions[J]. *Tourism Management*, 2019, 75: 353-369.
- [33] Tversky A, Kahneman D. Judgment under uncertainty: Heuristics and biases[J]. *Science*, 1974, 185(4157): 1124-1131.
- [34] Howley K. Understanding community media: SAGE publications[M]. Los Angeles: SAGE Publications, 2009.
- [35] Wakefield R. The influence of user affect in online information disclosure [J]. *Journal of Strategic Information Systems*, 2013, 22(2): 157-174.
- [36] Sundar S S, Kang H, Wu M, et al. Unlocking the privacy paradox: Do cognitive heuristics hold the key? [C]//CHI13 Extended Abstracts on Human Factors in Computing Systems. ACM, 2013: 811-816.
- [37] Deuker A. Addressing the privacy paradox by expanded privacy awareness - the example of context-aware services [C]//IFIP PrimeLife International Summer School on Privacy and Identity Management for Life. Springer, Berlin, Heidelberg, 2009: 275-283.
- [38] Flender C, Müller G. Type indeterminacy in privacy decisions: The privacy paradox revisited[C]//International Sym-

- posium on Quantum Interaction. Springer, Berlin, Heidelberg, 2012: 148-159.
- [39] Waldman A E. There is no privacy paradox: How cognitive biases and design dark patterns affect online disclosure [J]. *Current Opinion in Psychology*, 2019, 31: 105-109.
- [40] Song J H, Kim H Y, Kim S, et al. Effects of personalized e-mail messages on privacy risk: Moderating roles of control and intimacy [J]. *Marketing Letters*, 2016, 27(1): 89-101.
- [41] Christin D, Sánchez López P, Reinhardt A, et al. Share with strangers: Privacy bubbles as user-centered privacy control for mobile content sharing applications [J]. *Information Security Technical Report*, 2013, 17(3): 105-116.
- [42] Alhazov A, Csuhaj-Varj, Erzs, et al. Privacy concerns and information disclosure: An illusion of control hypothesis [J]. *Theoretical Computer Science*, 2009, 410(35): 3188-3197.
- [43] Christofides E, Muise A, Desmarais S. Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? [J]. *Cyberpsychology & Behavior: The impact of the Internet, Multimedia and Virtual Reality on Behavior and Society*, 2009, 12(3): 341-345.
- [44] Ke M. Ethical issues in the big data industry[J]. *MIS Quarterly Executive* 2015, 14(2): 67-85.
- [45] Jia H, Wisniewski P J, Xu H, et al. Risk-taking as a learning process for shaping teens online information privacy behaviors[C]//*Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*. ACM, 2015: 583-599.
- [46] Bandara R, Fernando M, Akter S. The privacy paradox in the data-driven marketplace: The role of knowledge deficiency and psychological distance[J]. *Procedia Computer Science*, 2017, 121: 562-567.
- [47] Baek Y M. Solving the privacy paradox: A counter-argument experimental approach[J]. *Computers in Human Behavior*, 2014, 38: 33-42.
- [48] Keith M J, Maynes C, Lowry P B, et al. Privacy fatigue: The effect of privacy control complexity on consumer electronic information disclosure[C]//*International Conference on Information Systems (ICIS 2014)*, Auckland, New Zealand, December. 2014, 4: 14-17.
- [49] Choi H, Park J, Jung Y. The role of privacy fatigue in online privacy behavior[J]. *Computers in Human Behavior*, 2018, 81: 42-51.
- [50] Agi B, Jullien N. Is the Privacy Paradox in fact rational? [J/OL]. [2019-03-10]. <http://ssrn.com/abstract=3109695>.
- [51] Utz S, Krämer N C. The privacy paradox on social network sites revisited: The role of individual characteristics and group norms[J/OL]. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 2009, 3(2): e2. [2019-03-10]. <http://cyber-psychology.eu/article/view/4223/3265>.
- [52] Blank G, Bolsover G, Dubois E. A new privacy paradox: Young people and privacy on social network sites[J/OL]. Prepared for the Annual Meeting of the American Sociological Association, 2014. [2019-03-10]. <http://ssrn.com/abstract=2479938>.
- [53] Taddicken M. The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure[J]. *Journal of Computer-Mediated Communication*, 2014, 19(2): 248-273.
- [54] Beldad A, Kusumadewi M C. Here's my location, for your information: The impact of trust, benefits, and social influence on location sharing application use among Indonesian university students[J]. *Computers in Human Behavior*, 2015, 49: 102-110.
- [55] Lutz C, Strathoff P. Privacy concerns and online behavior – not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses[J]. *Social Science Electronic Publishing*, 2014, 81-99.
- [56] Van Gool E, Van Ouytsel J, Ponnet K, et al. To share or not to share? Adolescents' self-disclosure about peer relationships on Facebook: An application of the Prototype Willingness Model[J]. *Computers in Human Behavior*, 2015, 44: 230-239.
- [57] Hull G. Successful failure: What Foucault can teach us about privacy self-management in a world of Facebook and big data [J]. *Ethics and Information Technology*, 2015, 17(2): 89-101.
- [58] 黄俊, 李晔, 张宏伟. 解释水平理论的应用及发展 [J]. *心理科学进展*, 2015, 23(1): 110-119.
- [59] Lynch Jr, John G, Zauberger G. Construing consumer decision making[J]. *Journal of Consumer Psychology*, 2007, 17(2): 107-112.

- [60] Sordi J D, Perin M G, Petrini M D C, et al. Construal level and collaborative consumption: An exploratory approach [J]. *International Journal of Consumer Studies*, 2018, 42(2): 264-273.
- [61] 李贺, 余璐, 许一明, 等. 解释水平理论视角下的社交网络隐私悖论研究 [J]. *情报学报*, 2018, 37(01): 1-13.
- [62] Wottrich V M, van Reijmersdal E A, Smit E G. The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns [J]. *Decision Support Systems*, 2018, 106: 44-52.
- [63] Buck C, Burster S, Eymann T. Cognitive biases and information privacy in mobile applications [J]. *Hmd Praxis Der Wirtschaftsinformatik*, 2018, 55(3): 646-658.
- [64] Zhou T. Examining mobile SNS continuance from a dual perspective of social capital and privacy concern [A] // *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications*. IGI Global, 2019: 1498-1514.
- [65] Hallam C, Zanella G. Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards [J]. *Computers in Human Behavior*, 2017, 68: 217-227.
- [66] Tussyadiah I, Li S, Miller G. Privacy protection in tourism: Where we are and where we should be heading for [C] // *Proceedings of the International Conference in Nicosia*. ICT, 2019: 278-290.
- [67] Gerber N, Gerber P, Volkamer M. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior [J]. *Computers & Security*, 2018, 77(0167-4048): 226-261.
- [68] Staddon J, Acquisti A, LeFevre K. Self-reported social network behavior: Accuracy predictors and implications for the privacy paradox [C] // *2013 International Conference on Social Computing*. IEEE, 2013: 295-302.
- [69] Miltgen C L, Peyrat-Guillard D. Cultural and generational influences on privacy concerns: A qualitative study in seven European countries [J]. *European Journal of Information Systems*, 2014, 23(2): 103-125.
- [70] Young A L, Quan-Haase A. Privacy protection strategies on facebook: The Internet privacy paradox revisited [J]. *Information Communication & Society*, 2013, 16(4): 479-500.
- [71] Peters A N, Winschiers-Theophilus H, Mennecke B E. Cultural influences on Facebook practices: A comparative study of college students in Namibia and the United States [J]. *Computers in Human Behavior*, 2015, 49: 259-271.
- [72] 曾伏娥, 邹周, 陶然. 个性化营销一定会引发隐私担忧吗: 基于拟人化沟通的视角 [J]. *南开管理评论*, 2018, 21(5): 83-92.
- [73] Komiak S Y X, Wang W, Benbasat I. Trust building in virtual salespersons versus in human salespersons: Similarities and differences [J]. *E-Service*, 2004, 3(3): 49-64.
- [74] Bilgic M, Mooney R J. Explaining recommendations: Satisfaction vs. promotion [C] // *International Conference on Intelligent User Interfaces*. IUI, 2005, 5: 153.
- [75] Jannach D, Zanker M, Felfernig A, et al. *Recommender systems: An introduction* [M]. Cambridge: Cambridge University Press, 2010.
- [76] Hassenzahl M, Schöbel M, Trautmann T. How motivational orientation influences the evaluation and choice of hedonic and pragmatic interactive products: The role of regulatory focus [J]. *Interacting with Computers*, 2008, 20(4-5): 473-479.
- [77] Mcsherry D. Explanation in recommender systems [J]. *Artificial Intelligence Review*, 2005, 24(2): 179-197.
- [78] 罗映宇. 个性化推荐解释、矛盾性追评对消费者在线购买决策的影响 [D]. 泉州: 华侨大学, 2019.
- [79] Kalai A, Wafa A, Zayani C A, et al. LoTrust: A social trust level model based on time-aware social interactions and interests similarity [C] // *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2016: 428-436.
- [80] Kim J K, Kim S H. Intention to disclose personal information in LBS: Based on privacy calculus perspective [J]. *The Journal of Information Systems*, 2012, 21(4): 55-79.
- [81] Li H, Wu J, Gao Y, et al. Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective [J]. *International Journal of Medical Informatics*, 2016, 88: 8-17.
- [82] Sarnikar S. *What can behavioral economics teach us about teaching economics?* [M]. Berlin: Springer, 2015.
- [83] 马庆国, 王小毅. 认知神经科学、神经经济学与神经管理学 [J]. *管理世界*, 2006, 10: 139-149.
- [84] GDPR 昨日生效! 欧盟推出史上最严个人隐私保护法, 违反罚 2000 万欧元 [EB/OL]. [2019-04-20]. <https://new.qq.com/omn/20180527/20180527A07FXV.html?pc>.

(收稿日期: 2019-08-14)