



沟通隐私管理理论整体视角下 移动用户信息披露决策的过程研究

刘百灵, 孙文静

华中师范大学 信息管理学院, 武汉 430079

摘要: 随着移动互联网和大数据的发展, 用户数据已成为企业拥有竞争优势的重要资源。然而, 移动服务商对用户数据的收集和使用引发了用户的隐私担忧。由于普遍存在的隐私悖论现象, 隐私问题对用户披露信息的阻碍作用变得扑朔迷离, 因此有必要更好地理解移动用户个人信息披露的本质。

基于沟通隐私管理理论的整体框架, 将用户信息披露决策的过程划分为认知因素、认知权衡和披露决策3个阶段, 认知因素包括感知的拥有、感知的监视、隐私价值倾向和隐私政策感知的有效性, 认知权衡包括隐私风险、隐私控制; 聚焦于移动用户的认知体验, 从移动用户隐私悖论的视角出发, 构建移动用户个人信息披露决策3阶段模型; 以移动商务为研究背景, 将信任和具体情景下的隐私担忧视作两种不同的态度, 评估两者对用户信息披露意愿的相互作用。采用问卷调查的方式收集样本数据, 运用 Smart PLS 3.0 对收集的 406 份有效数据进行实证分析, 以探究移动用户信息披露决策的过程。

研究表明, 用户信息披露决策的认知因素对认知权衡有显著的影响, 进而形成用户披露信息的积极态度和消极态度, 即信任和隐私担忧, 最终信任发挥关键的作用, 连同权衡结果共同影响个人信息披露决策, 即信息披露意愿。

应用沟通隐私管理理论的整体框架研究用户披露个人信息决策的过程, 深化了人们对移动用户个人信息披露决策产生过程的了解, 从理论上丰富了移动商务环境下用户信息披露行为的研究, 进一步证实了移动商务环境下的隐私悖论现象, 为隐私悖论现象提供了新的见解, 对移动服务商和移动商务应用开发商有针对性地采取措施以获取用户更多的个人信息具有一定的指导意义。

关键词: 沟通隐私管理理论; 移动商务; 信息披露; 感知的监视; 隐私悖论

中图分类号: F713.363

文献标识码: A

doi: 10.3969/j.issn.1672-0334.2021.06.009

文章编号: 1672-0334(2021)06-0076-12

引言

随着移动互联网和大数据的发展, 用户数据已成为企业拥有竞争优势的重要资源。相对于传统的网络环境, 在移动商务环境下, 用户享受移动服务带来便利的同时, 也增加了移动服务商获取更多敏感个人信息的机会, 如个人身份可识别信息、实时的地理

位置、财务信息、通讯录等。然而, 这种前所未有的获取用户大量信息的机会为移动隐私信息泄露敞开了大门^[1]。据 Gemalto 发布的 2016 年《数据泄露水平指数调查报告》显示, 在全球范围内, 2016 年已曝光的数据泄露事件高达 1 800 起, 这些事件导致近 14 亿条记录外泄, 平均每天高达 377 万条。日益突出的隐

收稿日期: 2018-02-03 **修返日期:** 2019-11-03

基金项目: 国家社会科学基金(20BGL283)

作者简介: 刘百灵, 工学博士, 华中师范大学信息管理学院副教授, 研究方向为信息系统、隐私保护和移动电子商务等, 代表性学术成果为“Achieving a balance between privacy protection and data collection: a field experimental examination of a theory driven information technology solution”, 在线发表在 2021 年《Information Systems Research》, E-mail: bl_liu@ccnu.edu.cn

孙文静, 华中师范大学信息管理学院硕士研究生, 研究方向为信息系统等, E-mail: 290204688@qq.com

私泄露问题引发了移动用户严重的隐私担忧, 从而降低其信息披露意愿^[2-3]。

据中国互联网络信息中心发布的《第44次中国互联网络发展状况统计报告》显示, 尽管大部分用户认为手机是泄露个人信息的重要载体, 但截至2019年6月, 手机网络购物用户规模达6.22亿, 2018年年底增长2 989万。这与人们在意隐私安全问题、谨言慎行、尽力保护自己的信息并拒绝披露个人信息的理论相悖^[4]。这一矛盾现象称为隐私悖论, 即一方面用户担心自身的隐私遭到侵犯, 但另一方面为享受移动服务带来的便利而随意地披露个人信息^[5-6]。该现象使移动用户的信息披露行为变得扑朔迷离^[7-8], 阻碍了移动企业持续健康地发展, 因此有必要对移动商务环境下用户个人信息披露的本质展开全面深入的研究。已有研究主要集中于隐私计算理论, 探索移动用户信息披露意愿的前置因素, 鲜有研究基于移动用户的认知体验, 结合移动用户隐私悖论的现象, 聚焦于用户认知体验的认知因素、认知权衡和披露决策3个阶段的探究。这也正是国际上信息系统领域的学者强烈呼吁开展研究的问题^[9]。移动服务商要想获取用户更多的个人信息, 有必要了解移动用户信息披露的本质, 这也是学界和业界都比较关注的问题。

沟通隐私管理 (communication privacy management, CPM) 理论解释了人们进行信息披露决策的过程^[10], 且CPM理论已被广泛用于解决信息系统领域中的隐私问题^[11-12]。因此, 本研究基于CPM的整体视角, 对用户披露个人信息决策的过程中认知体验的3个阶段展开全面的探究, 构建个人信息披露决策模型, 并以移动商务为具体情景进行实证分析, 不仅可以为理解移动用户披露信息的本质提供理论基础, 丰富移动商务环境下用户信息披露行为的研究, 也有助于为移动服务商获取用户更多个人信息提供有意义的指导和借鉴。

1 相关研究评述

移动商务环境具有移动性、便利性和个性化等独特属性^[13], 使隐私悖论现象尤为突出。当前对移动商务环境下用户信息披露意愿的研究也在不断深入和升华, 且主要从隐私计算理论的视角揭示隐私悖论的形成原因。KEITH et al.^[14]基于社会认知理论, 采用对比实验的方式, 验证隐私自我效能对移动用户的信任、感知风险、感知利益和信息披露行为的影响; WANG et al.^[2]运用隐私计算理论, 通过移动应用程序提出并验证了影响感知利益和感知风险双重路径的因素, 发现用户感知风险降低其披露地理位置的意愿, 但感知利益 (如个性化服务和自我表现力) 对用户披露位置信息有更大的促进作用; 刘百灵等^[15]基于隐私计算理论, 从沉浸理论视角出发, 探究移动购物用户持续使用意愿的影响因素, 研究发现, 移动购物用户通过权衡隐私担忧与信任, 以决策其信息披露行为, 并间接影响其持续使用意愿。

然而, 随着研究进一步深入, 相对于隐私计算理论, CPM理论更全面、系统地解决了信息管理领域中的隐私问题^[11]。CPM理论将隐私比喻为一个从自我到他人的具有弹性 (从开放到封闭) 的边界, 并将隐私边界看成是一个从完全开放到完全封闭的连续体。该理论提出了人们管理个人隐私边界的5条准则^[16], 分别为个人信息的拥有权、个人信息的控制权、隐私边界规则、隐私边界协作和隐私边界混乱。XU et al.^[9]运用CPM理论的第3条~第5条准则, 通过对比研究电子商务网站、社交网站、金融网站和健康网站4种环境下个人隐私感知与组织隐私保护措施之间的关系, 揭示了不同环境下隐私担忧的形成原因; CHANG et al.^[17]基于CPM理论的第3条~第5条准则, 从隐私政策的通知、访问和实施3个维度出发, 深入探究在线银行环境下用户感知的隐私, 并阐述了消费者对隐私边界的制定和管理情况; CHOI et al.^[3]基于CPM理论的第1条准则, 提出信息收集和个人信息发布控制权是移动应用中威胁信息所有权的两种隐私特征, 这两种隐私特征增加用户具体情景下的隐私担忧, 继而降低其向Facebook应用提交个人信息的意愿。

综上所述, 已有研究侧重于从隐私计算的视角解释隐私悖论, 然而基于CPM理论视角的研究非常有限, 尤其缺乏涉及财务交易等敏感信息的移动商务环境下的研究, 并且已有研究仅应用CPM的部分准则探讨信息隐私的相关问题。而PETRONIO^[10]通过对CPM理论的分析发现, 要想理解信息披露的本质, 需要全面考虑CPM理论中隐私边界管理的所有准则。因此, 本研究从CPM理论的整体视角出发, 结合隐私悖论现象, 以移动商务为具体情景, 探求移动用户个人信息披露决策的过程, 以期从本质上对移动用户信息披露的影响机理提供全面的了解, 为移动服务商更好地收集用户个人信息提供相应的启发和建议。

2 研究假设和模型构建

2.1 研究假设

2.1.1 信息披露决策的认知因素

CPM理论第1条准则是个人信息的拥有权^[16]。CPM理论认为人们持有一种感知的所有权, 并有权处理个人信息, 即决定打开边界披露个人信息, 或关闭边界隐藏个人信息。因此, 在移动商务环境下, 当移动服务商向用户索要个人信息时, 如果用户感知其个人信息是属于自己的, 即使他们的个人信息已经提供了服务商, 仍然希望持有对隐私边界的拥有权。心理所有权理论认为, 感知的拥有是一种基于认知的信念^[18], 映射了人们的3种动机, 即效能、自我认同和归属感^[19], 并以此为准则进行行为决策。因此, 本研究将感知的拥有作为信息披露的认知因素, 研究用户向移动服务商提供个人信息所感知的拥有权。

CPM理论的第2条准则是个人信息的控制权, 即

认为人们相信个人信息是属于自己的,因此假定有权控制这些信息^[16]。在不同的情况下,人们对隐私边界控制水平的要求是不同的。对隐私边界有较高的控制要求时,隐私边界的渗透性较低,则他人获得的信息非常有限,以保护个人信息^[20];反之,隐私边界具有较高的信息渗透性^[16],可能被他人收集到较多的个人信息,因而产生被监视的感觉^[12]。这种感知的监视可能会影响人们控制隐私边界的水平,因此,本研究通过感知的监视研究移动用户对隐私边界的控制水平,反映了个人信息的控制权。

CPM理论的第3条准则认为人们打开或隐匿隐私边界的抉择与其保持个人隐私边界的动机相关^[16]。XU et al.^[8]提出了隐私价值倾向的概念,即个人保护其隐私信息空间或者限制个人信息披露的一般倾向,作为一种保护个人隐私的动机,反映人们想要保持隐私边界的心理需要。如果移动用户将个人隐私看得很重要,其保持隐私边界的需求会非常强烈,隐私边界不易被打开。因此,本研究考虑隐私价值倾向对用户信息披露认知所产生的影响。

CPM理论的第4条准则认为,当个人信息被披露后,信息的所有者和信息的接收者共同拥有这些信息,并共同控制信息的使用,有共同的责任保证信息的隐私安全,即隐私边界协作^[16]。同时,CPM理论第5条准则也指出,当隐私边界协作机制出现错误或发生隐私侵犯,隐私边界管理会出现混乱^[16],人们希望有相关的措施来保护自己的隐私。隐私政策被认为是一种隐私边界协作机制,它使收集用户大量信息的服务商成为信息的监护者,并且有责任保证信息的安全^[9,17]。隐私边界协作与隐私边界混乱相互作用,使人们形成了对隐私政策有效性的认识^[17]。因此,本研究通过移动用户对隐私政策感知的有效性反映隐私边界的协作和混乱。

2.1.2 从信息披露决策认知因素到认知权衡

CPM理论认为人们是基于信息披露的风险与收益的权衡结果决定是否打开个人的隐私边界,即是否披露个人信息。与已有研究类似^[21-22],本研究通过隐私控制和隐私风险反映移动用户认知权衡的两个重要因素,并将隐私控制定义为一种感知的概念,它反映了用户认为自己有能力管理个人信息的披露和分享的一种信念;将隐私风险定义为对披露个人信息的预期损失,是对潜在的负面结果产生的不确定性。

如前所述,感知的拥有是对心理上认为属于自己的东西的一种占有和控制欲望^[23]。CPM理论认为,用户对其个人信息的占有欲愈强,就愈会担心个人信息流出隐私边界,其控制信息的欲望愈强^[16]。日新月异的信息技术给移动服务商提供了更加便利的监控手段^[1],使用户的个人信息的(如地理位置信息、行为偏好数据等)更容易被移动服务商收集和记录,从而提高了其被监视的感知^[11]。因此,移动用户迫切渴望控制自己的个人信息。然而,用户对其个人信息的控制愈强,对其管理信息能力的要求也就越高^[24],

越会对当前已有的控制水平感到不满,其感知的控制则相对较低^[25]。因此,本研究提出假设。

H₁ 移动用户对个人信息感知的拥有正向影响其感知的监视。

H₂ 移动用户对个人信息感知的拥有负向影响其感知的隐私控制。

感知的监视是指移动用户对他人观察、听取和记录其个人信息感到担忧的心理^[11]。随着互联网和信息技术的普及,移动技术快速发展。在移动商务环境中,服务商能利用各种先进的技术跟踪移动用户,收集其更多的敏感信息,这种对用户的监视行为通常是各种隐私风险的起源^[12]。频繁发生的数据泄露事件进一步引发人们对移动服务商数据监视程度的质疑,以及对随之而来的隐私风险的关注^[26]。当用户感知到移动服务商收集了自己过多的信息,即过多的信息离开了其隐私边界,便会更加觉得无法控制自己的信息,增加隐私损失的风险。因此,本研究提出假设。

H_{3a} 移动用户感知的监视负向影响其感知的隐私控制。

H_{3b} 移动用户感知的监视正向影响其感知的隐私风险。

用户的隐私价值倾向在社交网络环境下对感知的隐私控制有显著的负向影响,在电子商务网站、社交网站、金融网站和健康网站中对感知的隐私风险有显著的正向影响^[9]。而移动商务环境下,服务商更能轻易收集用户大量的敏感信息。因此,移动用户想要控制个人信息的难度更大,面临的隐私风险更多。倘若移动用户对个人隐私越重视,其对隐私控制的要求也就越高,其感知到的隐私控制则相对较低,而对隐私风险的感知相对较高^[25]。因此,本研究提出假设。

H_{4a} 移动用户的隐私价值倾向负向影响其感知的隐私控制。

H_{4b} 移动用户的隐私价值倾向正向影响其感知的隐私风险。

隐私政策是用来告知用户服务商将如何处理他们的个人信息,隐私政策感知的有效性表示移动用户对在线张贴的隐私声明可靠性的一种信任程度。目前,大部分移动用户根据服务商的相关声明判定该隐私规则是否符合自己的隐私目标,从而做出相应的信息披露决策^[27]。研究表明,服务商提供有效的隐私政策能显著提高消费者感知的隐私控制;同样地,服务商主动告知用户将如何处理其个人信息,能极大地降低信息披露带来的隐私风险^[17]。在基于位置的服务中,有学者发现隐私政策作为行业自律的一种有效隐私保护措施,能显著提高消费者对个人信息感知的控制^[28],对感知的隐私风险有显著的负向影响^[29]。因此,本研究提出假设。

H_{5a} 移动用户对隐私政策感知的有效性正向影响其感知的隐私控制。

H_{5b} 移动用户对隐私政策感知的有效性负向影响

其感知的隐私风险。

2.1.3 从信息披露认知权衡到决策

基于理性行为理论, 本研究将隐私担忧作为一种消极的态度, 将信任作为一种积极的态度, 二者共同影响移动用户信息披露的最终决策^[30]。已有研究证实, 隐私担忧和信任是权衡其信息披露行为的主要因素^[14-15]。刘百灵等^[15]探究移动购物用户持续使用意愿的影响因素, 发现移动用户通过权衡隐私担忧与信任, 以做出其信息披露行为的决策。依据 XU et al.^[22]的研究中对隐私担忧的理解, 本研究将隐私担忧定义为: 移动商务环境下, 用户对其可能失去隐私权的一种担忧; 依据林家宝等^[13]的研究中对信任的理解, 本研究将信任定义为: 移动用户对服务商在保护个人隐私信息方面的可依赖程度。

已有研究发现, 用户对个人信息控制感知能够显著降低隐私担忧^[28]。如果用户缺乏对个人信息的控制感知, 就会降低其对服务商的信任^[31]。当用户感知自己可以完全控制个人信息的处理情况, 能显著缓解他们的隐私担忧。在这种情况下, 用户会更愿意信任服务商, 并且提高个人的信息披露意愿^[25,32]。移动商务环境下, 用户可以随时随地使用移动服务, 同时他们大量的个人信息也被移动服务商收集。因此, 本研究认为用户对已披露给移动服务商的信息所感知的隐私控制对其隐私担忧、信任和个人信息的披露意愿起重要的作用。因此, 本研究提出假设。

H_{6a} 移动用户感知的隐私控制负向影响其隐私担忧。

H_{6b} 移动用户感知的隐私控制正向影响其对移动服务商的信任。

H_{6c} 移动用户感知的隐私控制正向影响其个人信息披露意愿。

CPM 理论认为, 用户的信息披露必然涉及到风险。SHARMA et al.^[11]基于社会化商务环境的研究发现, 用户感知的隐私风险对用户披露信息的意愿有显著的负向影响。类似地, 在移动商务环境下, 一旦用户的个人信息被服务商收集, 就可能存在个人隐

私泄露的风险。因此, 当用户在披露个人信息时, 会自主进行隐私风险评估。如果用户感知到隐私风险系数较高, 则会极大程度地增加其隐私担忧, 降低个人信任程度^[33-34], 从而影响其信息披露意愿^[16]。因此, 本研究提出假设。

H_{7a} 移动用户感知的隐私风险正向影响其隐私担忧。

H_{7b} 移动用户感知的隐私风险负向影响其对移动服务商的信任。

H_{7c} 移动用户感知的隐私风险负向影响其信息披露意愿。

一般而言, 用户的信息披露意愿与其对隐私的态度相关^[35]。个人隐私顾虑越高, 信息披露行为就会越谨慎^[36]。朱侯^[37]基于效用最大化和期望价值等理论, 研究发现信任会影响隐私担忧与个体隐私结果变量之间的关系。信任不仅能在很大程度上提升用户的行为意愿^[38], 同时还会受到隐私顾虑的负向影响^[32]。在传统的电子商务环境下, 大量研究表明, 用户的隐私担忧显著降低用户的信息披露意愿, 信任对信息披露意愿有显著的正向作用, 并且隐私担忧对信任有显著的负向影响^[39-40]。而在移动商务环境下, 用户的隐私担忧更加突出, 信任成为移动用户产生行为动机的关键因素, 显著影响用户信息披露意愿^[41-42]。因此, 本研究提出假设。

H_{8a} 移动用户的隐私担忧负向影响其对移动服务商的信任。

H_{8b} 移动用户的隐私担忧负向影响其信息披露意愿。

H₉ 移动用户的信任正向影响其信息披露意愿。

2.2 模型构建

基于 CPM 理论, 以移动商务为具体情景, 本研究构建移动商务环境下用户披露个人信息的决策模型, 将个人披露信息决策的过程分为 3 个阶段, 分别为信息披露决策的认知因素、认知权衡和披露决策。移动用户会依据最近的经历和了解的信息, 不断重复以上过程。研究模型见图 1。

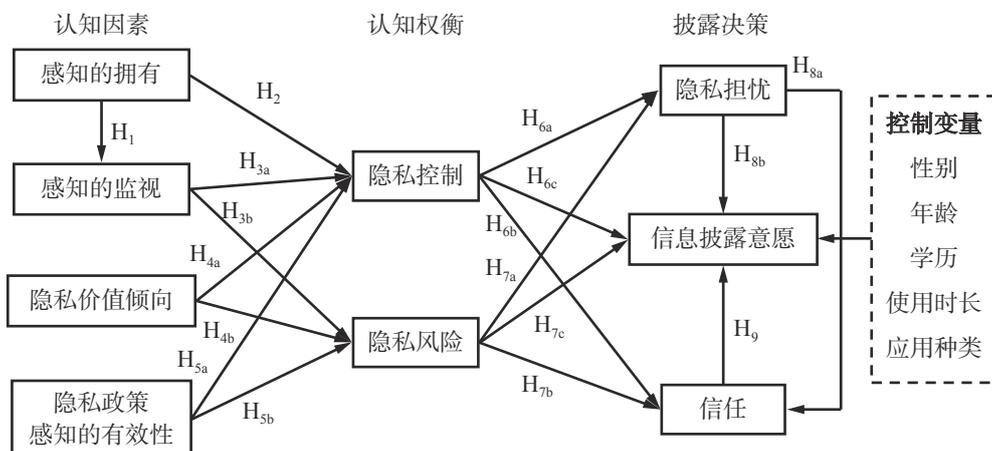


图 1 移动商务环境下用户个人信息披露决策模型

Figure 1 Model of Users' Personal Information Disclosure Decision in Mobile Commerce Environment

3 研究设计

3.1 问卷设计

本研究借鉴国内外研究中的成熟量表设计问卷,并适当调整措辞以适用于本研究。为了提高问卷的内容效度,邀请3位本领域专家对初始量表进行审阅。采用修改后的问卷进行小规模的前测,主要采用线下纸质问卷的方式,邀请80名有移动商务交易活动经历的在校大学生,于2017年2月21日开始,3月7日结束,历时15天,收回79份有效问卷,并根据分析结

果对题项进行调整,最终形成正式问卷。

正式问卷分为3个部分:第1部分为个人基本信息,包括被试的人口统计信息和移动商务应用的使用情况等控制变量;第2部分用于检测与情景无关的核心变量,即隐私价值倾向;第3部分用于检测基于具体移动商务情景的核心变量,即感知的拥有、感知的监视、隐私政策感知的有效性、隐私控制、隐私风险、隐私担忧、信任、信息披露意愿,详见表1。除第1部分采用一般性选择题外,其他部分均采用Likert 7点

表1 测量指标
Table 1 Measure Items

变量	代码	题项
感知的拥有 (PO)	PO ₁	使用该移动商务应用进行交易时,我觉得我提供的信息是属于我自己的
	PO ₂	使用该移动商务应用进行交易时,我感觉对自己提供的信息拥有高度的个人所有权
	PO ₃	使用该移动商务应用进行交易时,我觉得我提供的信息是个人的
	PO ₄	使用该移动商务应用进行交易时,我相信我披露的信息是属于我的
感知的监视 (PS)	PS ₁	我觉得该移动商务应用可能会通过我使用的移动设备监视我的地理位置
	PS ₂	我觉得该移动商务应用收集了我很多信息
	PS ₃	该移动商务应用可能会记录我在移动设备上的各种活动和操作
隐私价值倾向 (Dtv)	Dtv ₁	我比一般人把保护个人隐私看得更重要
	Dtv ₂	我对移动商务应用处理我个人信息的方式比一般人感到更敏感
	Dtv ₃	相对一般人而言,移动商务应用对我个人信息的潜在威胁,我较少担心
隐私政策感知的有效性 (Epp)	Epp ₁	我相信该移动商务应用隐私声明是他们对保护我个人信息的承诺
	Epp ₂	有了该移动商务应用隐私声明,我认为该移动服务商将会保证我个人信息的隐私和安全
	Epp ₃	我相信该移动商务网站的隐私声明是一种证明他们承诺保护用户隐私的有效方式
隐私控制 (PC)	PC ₁	我觉得我能控制:我的何种信息被该移动商务应用公布
	PC ₂	我觉得我无法控制:谁可以访问该移动商务应用收集的我的个人信息
	PC ₃	我觉得我能控制:该移动商务应用如何使用我的个人信息
	PC ₄	我觉得我能控制:已经提供给该移动商务应用的个人信息
隐私风险 (PR)	PR ₁	向该移动商务应用提供个人信息具有较大的风险
	PR ₂	向该移动商务应用提供个人信息很有可能带来较大的隐私损失
	PR ₃	该移动商务应用可能不适当地使用个人信息
	PR ₄	向该移动商务应用提供个人信息将会带来许多预料不到的问题
隐私担忧 (Pco)	Pco ₁	我担心我提供给该移动商务应用的信息可能会被滥用
	Pco ₂	我担心其他服务商或用户能够在该移动商务应用上找到我的隐私信息
	Pco ₃	向该移动商务应用提供我的个人信息时,其他服务商或用户可能处理或使用这些信息,这让我感到担心
	Pco ₄	向该移动商务应用提供我的个人信息时,这些信息很可能被以某种我无法预知的方式使用,这让我感到担心
信任 (Tru)	Tru ₁	我相信该移动服务商会告诉我有关我提供的个人信息的实情,并且遵守它的承诺
	Tru ₂	我相信该移动服务商在处理我个人信息时会随时考虑到我的利益
	Tru ₃	我相信该移动服务商会很诚实地处理我提供的个人信息
	Tru ₄	我认为该移动服务商在处理我提供的个人信息方面是值得信赖的
信息披露意愿 (Wdi)	Wdi ₁	使用该移动商务应用购买商品或服务,需要我提供精确的可识别信息
	Wdi ₂	使用该移动商务应用需要我提供准确的注册信息,其中可能包括银行卡信息
	Wdi ₃	在该移动商务应用上进行交易时,需要我提供支付账号信息

评分法, 1为非常不同意或非常不愿意, 7为非常同意或非常愿意。

问卷量表中, 借鉴 SHARMA et al.^[11] 测量感知拥有和感知监视的量表, 本研究设计4个题项测量感知的拥有, 设计3个题项测量感知的监视; 借鉴 XU et al.^[9] 测量隐私价值倾向和隐私政策感知的有效性的量表, 本研究设计3个题项测量隐私价值倾向, 设计3个题项测量隐私政策感知的有效性; 测量隐私控制的题项改编自 XU et al.^[22] 测量信息控制的量表, 本研究设计4个题项; 借鉴 XU et al.^[21] 测量隐私风险的题项的题项, 本研究设计4个题项测量隐私风险; 采用 GU et al.^[43] 编制的“具体情景下隐私担忧”测量隐私担忧的题项, 包括4个题项; 以林家宝等^[13] 测量信任的题项为量表, 本研究设计4个题项测量信任; 根据 DINEV et al.^[44] 测量“在线交易信息披露意愿”变量的量表, 本研究改编后用3个题项测量信息披露意愿。各变量的测量题项见表1。

3.2 数据收集

正式问卷有纸质问卷和电子问卷两种。纸质问卷面向高校大学生, 因为大学生是移动用户的主体, 高素质的学生样本比较具有代表性; 通过问卷星发放电子问卷, 调查对象面向全国各地。由于问卷第3部分需要被试基于具体移动商务应用情景填写, 因此采用被试情景回忆的方式。首先, 请被试填写最近3个月中使用最频繁的一种移动商务应用, 并向被试解释移动商务及其应用的定义; 其次, 根据被试填写的移动商务应用, 请他们回忆最近3个月使用该移动商务应用的经历, 并根据此经历填写问卷。填写结束后, 请被试抽取红包或礼品。

问卷调查于2017年3月20日开始, 5月15日结束, 历时56天, 共收集509份问卷, 纸质问卷209份,

电子问卷300份。按照以下原则进行有效问卷的筛选: ①删除使用移动商务应用不足6个月的问卷; ②删除最近1个月从未使用移动商务应用进行交易的问卷; ③删除填写不完整的问卷; ④删除有规律作答的问卷。最终得到406份有效问卷, 问卷有效回收率为79.764%, 符合统计分析的标准。被试的基本人口统计特征见表2。

由表2可知, 被试的男女比例基本趋于均衡, 男性占42.857%, 女性占57.143%; 年龄集中在18岁~29岁, 占80.296%, 说明被试以成年年轻人为主, 符合中国移动网民年龄集中的分布区间; 91.626%的被试为本科及以上学历, 表明调查对象大部分具有较高的文化水平; 使用移动购物应用的时间为2年及以上的人数居多, 约占77.832%, 说明大部分被试对于移动商务应用较为熟悉, 有助于保证问卷的质量。

表3为数据的描述性统计结果, 各指标均值的范围为3.296~5.786, 表明样本数据分布均衡; 标准差的范围为1.087~1.540, 说明样本数据离散程度低。本研究样本数据偏度绝对值的最大值为1.346, 峰度绝对值的最大值为2.000。综上所述, 可以认为样本数据基本服从正态分布标准。

由于问卷由被试一人独立完成, 因此有必要考虑共同方法偏差问题。本研究在问卷设计阶段就设置了两个反向问题, 以预防同源方法偏差的影响。采用 Harman 单因子检验方法, 对回收的问卷进行同源方法偏差检验^[39]。对所有变量进行未旋转的探索性因子分析, 结果表明, 所有指标的非旋转因子分析没有出现一个主导的单因子, 第1个因子只解释了25.550%的方差变异, 表明此次调查几乎不受同源方法偏差的影响。

多重共线性检验结果表明, 容差均大于0.100, 共

表2 人口统计特征

Table 2 Demographic Characteristics

人口统计变量		频数	百分比/%	人口统计变量		频数	百分比/%
性别	男	174	42.857	教育程度	大专及以下	34	8.374
	女	232	57.143		本科	208	51.232
年龄	18岁以下	4	0.985		硕士	143	35.222
	18岁~24岁	244	60.099		博士及以上	21	5.172
	25岁~29岁	82	20.197	应用种类	手机淘宝	98	24.138
	30岁~39岁	57	14.039		手机天猫	5	1.232
	40以上	19	4.680		手机京东	17	4.187
使用移动商务应用时间	1年以下	29	7.143		支付宝	249	61.330
	1年~2年	61	15.025		手机银行	10	2.463
	2年~3年	91	22.414	大众点评	7	1.724	
	3年~4年	90	22.167	其他	20	4.926	
	4年以上	135	33.251				

表3 描述性统计结果

Table 3 Results for Descriptive Statistics

变量	代码	均值	标准差	偏度	峰度
感知的拥有 (PO)	PO ₁	5.643	1.196	-1.346	2.000
	PO ₂	5.746	1.224	-1.316	1.610
	PO ₃	5.786	1.131	-1.257	1.574
	PO ₄	5.623	1.192	-1.024	0.948
感知的监视(PS)	PS ₁	5.308	1.294	-0.986	0.703
	PS ₂	5.692	1.087	-1.173	1.626
	PS ₃	5.584	1.140	-1.101	1.669
隐私价值倾向 (Dtv)	Dtv ₁	5.377	1.382	-0.761	0.065
	Dtv ₂	5.074	1.380	-0.558	-0.191
	Dtv ₃	4.899	1.363	-0.698	0.052
隐私政策感知的 有效性(Epp)	Epp ₁	4.833	1.317	-0.724	-0.011
	Epp ₂	4.500	1.368	-0.396	-0.506
	Epp ₃	4.638	1.355	-0.536	-0.319
隐私控制 (PC)	PC ₁	3.485	1.482	0.468	-0.620
	PC ₂	3.296	1.451	0.557	-0.478
	PC ₃	3.300	1.322	0.621	-0.105
	PC ₄	3.552	1.428	0.455	-0.559
隐私风险 (PR)	PR ₁	4.823	1.262	-0.425	-0.258
	PR ₂	4.872	1.270	-0.579	-0.062
	PR ₃	4.909	1.266	-0.509	-0.123
	PR ₄	4.892	1.336	-0.437	-0.446
隐私担忧 (Pco)	Pco ₁	5.101	1.254	-0.637	0.045
	Pco ₂	5.214	1.170	-0.749	0.677
	Pco ₃	5.182	1.212	-0.848	0.643
	Pco ₄	5.303	1.198	-0.825	0.706
信任(Tru)	Tru ₁	4.246	1.340	-0.228	-0.415
	Tru ₂	3.963	1.385	-0.040	-0.513
	Tru ₃	4.044	1.349	-0.087	-0.472
	Tru ₄	4.175	1.319	-0.170	-0.299
信息披露意愿 (Wdi)	Wdi ₁	4.224	1.540	-0.205	-1.017
	Wdi ₂	4.017	1.500	-0.078	-0.981
	Wdi ₃	4.303	1.467	-0.346	-0.712

表4 量表的信度和效度

Table 4 Reliability and Validity of the Scales

因子	指标	标准负荷	AVE	CR	Cronbach's α
PO	PO ₁	0.847	0.766	0.929	0.898
	PO ₂	0.893			
	PO ₃	0.911			
	PO ₄	0.848			
PS	PS ₁	0.832	0.712	0.881	0.797
	PS ₂	0.892			
	PS ₃	0.805			
Dtv	Dtv ₁	0.909	0.771	0.910	0.857
	Dtv ₂	0.920			
	Dtv ₃	0.801			
Epp	Epp ₁	0.886	0.811	0.928	0.884
	Epp ₂	0.919			
	Epp ₃	0.896			
PC	PC ₁	0.761	0.722	0.912	0.872
	PC ₂	0.898			
	PC ₃	0.898			
	PC ₄	0.835			
PR	PR ₁	0.880	0.781	0.935	0.907
	PR ₂	0.890			
	PR ₃	0.881			
	PR ₄	0.884			
Pco	Pco ₁	0.881	0.785	0.936	0.909
	Pco ₂	0.888			
	Pco ₃	0.880			
	Pco ₄	0.896			
Tru	Tru ₁	0.871	0.792	0.939	0.913
	Tru ₂	0.877			
	Tru ₃	0.902			
	Tru ₄	0.910			
Wdi	Wdi ₁	0.912	0.832	0.937	0.900
	Wdi ₂	0.928			
	Wdi ₃	0.897			

线性诊断方差膨胀因子均小于 $10^{[45]}$,说明不存在共线性问题。

4 实证结果分析

4.1 信度和效度检验

本研究采用验证性因子分析对题项的信度和效度进行检验,结果见表4。各变量的Cronbach's α 值

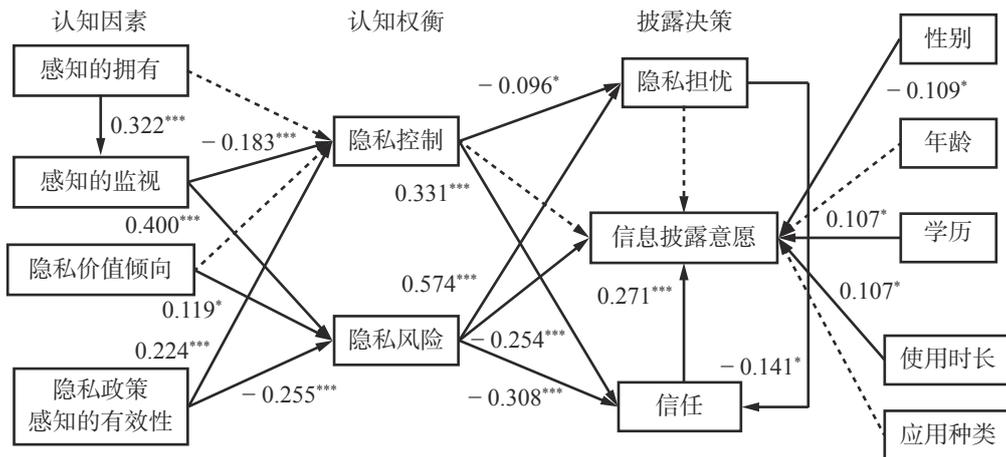
和复合信度(CR)都大于0.700,表明量表具有较好的信度;标准负荷均大于0.700,且均在0.010的水平上显著;各因子的平均方差抽取(AVE)值均高于阈值0.500,表明量表具有较好的收敛效度。

通过比较各变量AVE值的平方根和变量之间的相关系数的大小,进一步检验判别效度,检验结果见表5,各变量AVE值的平方根均大于相应的相关系数,

表5 相关系数
Table 5 Correlation Coefficients

	<i>PO</i>	<i>PS</i>	<i>Dtv</i>	<i>Epp</i>	<i>PC</i>	<i>PR</i>	<i>Pco</i>	<i>Tru</i>	<i>Wdi</i>
<i>PO</i>	0.875								
<i>PS</i>	0.332	0.844							
<i>Dtv</i>	0.338	0.243	0.878						
<i>Epp</i>	0.080	-0.081	0.080	0.901					
<i>PC</i>	-0.059	-0.201	0.002	0.239	0.850				
<i>PR</i>	0.144	0.450	0.196	-0.278	-0.076	0.884			
<i>Pco</i>	0.251	0.401	0.287	-0.255	-0.139	0.581	0.886		
<i>Tru</i>	0.008	-0.226	0.093	0.623	0.374	-0.415	-0.366	0.890	
<i>Wdi</i>	0.054	-0.003	0.063	0.277	0.095	-0.307	-0.194	0.341	0.912

注: 对角线上的数据为各变量AVE值的平方根。



注: ***为 $p < 0.001$, **为 $p < 0.010$, *为 $p < 0.050$; 虚线表示不显著。

图2 研究模型假设检验结果

Figure 2 Hypothesis Testing Results for the Research Model

表明变量具有良好的判别效度。

4.2 假设检验

本研究采用 Smart PLS 3.0 对假设进行检验, 模型的检验结果见图 2。

(1) 移动商务环境下, 用户披露个人信息决策的过程经历了 3 个阶段, 具体来说, 用户对个人信息所感知的拥有、对服务商感知的监视、对保护个人信息隐私的需求和对服务商提供的隐私保护措施, 共同影响他们对隐私控制与隐私风险的权衡, 进而形成积极或消极的态度, 即对移动服务商的信任和对个人信息的隐私担忧, 最终信任发挥关键作用, 直接影响用户披露个人信息的决策。这一结果, 支持了已有大部分研究观点, 而隐私担忧通过信任对用户披露信息的意愿产生间接的消极影响。

(2) 在影响移动用户披露个人信息的认知权衡因

素中, 发现感知的监视和隐私政策感知的有效性对隐私控制产生显著的影响, 即 H_{3a} 和 H_{5a} 得到验证; 感知的监视、隐私价值倾向和隐私政策感知的有效性对隐私风险产生显著的影响, 即 H_{3b} 、 H_{4b} 和 H_{5b} 得到验证, 并且感知的监视对隐私风险的影响最大, 路径系数达到 0.400, 说明移动商务应用过多收集用户的个人信息是引发隐私风险感知的主要因素, 隐私政策能够在一定程度上缓解用户感知的隐私风险, 提高其隐私控制感知。

然而, 本研究发现用户对个人信息感知的拥有与隐私控制之间无直接的显著关系, 而是通过感知的监视间接影响隐私控制, 并且用户的隐私价值倾向对感知的隐私控制也没有显著的影响, 即 H_1 得到验证, H_2 和 H_{4a} 未得到验证, 这与 XU et al.^[9] 的研究结果一致。可能是因为在当前的移动商务环境下, 无论

用户是否认为个人信息属于自己, 无论是否重视隐私保护, 当用户将个人信息披露给移动服务商之后, 其没有途径获悉并控制这些信息将会被如何使用以及被谁访问等后续使用情况, 这与感知的隐私控制因子得分较低一致, 即说明感知的拥有和隐私价值倾向对隐私控制无显著的影响。

(3) 移动用户对信息披露的认知权衡中, 隐私控制和隐私风险均对隐私担忧和信任产生显著的影响, 即对个人信息的控制能够缓解用户的隐私担忧, 提高其对移动服务商的信任, 相反地, 隐私风险会增加用户的隐私担忧, 降低其对移动服务商的信任, 因此, H_{6a} 、 H_{6b} 、 H_{7a} 和 H_{7b} 得到验证。隐私风险对信息披露意愿具有显著的负向影响, 但隐私控制对信息披露意愿没有直接的显著影响, 即 H_{7c} 得到验证, H_{6c} 未得到验证, 这可能是因为移动用户微弱的隐私控制感知对个人信息披露的影响被信任抵消。感知的隐私控制和信任均为消费者对待个人信息披露的正面态度, 前者强调能力, 后者更着重强调信念。如前所述, 目前中国常用的移动商务应用一般没有给予用户较多的隐私控制措施, 导致移动用户的隐私控制意识一直较为薄弱, 再加上本研究的被试选择的具体情景都是基于支付宝、手机淘宝等信任度较高的移动商务应用, 因此, 相对于在目前有限的隐私控制措施下认为自己有能力控制其个人信息而言, 信任的作用显得尤为突出, 很大程度上弥补了用户严重缺乏隐私控制权的不足。综上, 隐私控制的感知对个人信息披露意愿的影响作用不显著。

(4) 在信息披露决策的过程中, 信任显著地正向影响个人信息披露意愿, 隐私担忧对个人信息披露意愿无显著的直接作用, 而是通过信任影响个人信息披露意愿, 即 H_{8a} 和 H_9 得到验证, 但 H_{8b} 未得到验证, 这与已有研究相悖。可能是因为前人的研究主要针对传统的网络环境, 而本研究聚焦于隐私问题较为严重的移动商务环境, 研究背景存在较大差异。这一结果证实移动商务环境下普遍存在隐私悖论现象^[3], 也进一步揭示了移动商务环境下隐私悖论产生的原因, 即随着移动商务的流行及其提供的便利, “羊群效应”很好地诠释了大多数移动用户的心理。迫于当前的环境趋势, 用户别无选择, 无论其是否重视自己的隐私, 为顺应潮流, 获得使用机会, 只能选择加入信任度较高的移动商务应用。因此, 隐私悖论可能是用户一种无奈的外在表现, 尤其在涉及用户大量敏感个人信息的移动环境下, 用户认为或许通过选择信任度较高的移动服务商还能保障个人信息的安全。至此, 隐私悖论现象也对移动服务商和移动应用开发商提出了一个非常严肃的问题。

(5) 通过对控制变量的研究发现, 在移动商务环境下, 用户的学历水平越高, 其使用移动商务应用的年限越久, 其披露个人信息的意图越明显, 且不同性别的用户群体对于披露隐私信息的态度存在一定的差异, 男性用户群体可能更偏向于提供个人信息, 女性则反之, 这与 KOCK et al.^[45] 的研究结果一致。

5 结论

5.1 研究结果

本研究基于 CPM 理论, 构建移动环境下用户披露个人信息的决策模型, 并以移动商务为具体情景对该模型进行验证。研究结果表明, 用户披露个人信息的决策过程经历了认知因素、认知权衡和披露决策 3 个阶段, 认知因素包括感知的拥有、感知的监视、隐私价值倾向和隐私政策感知的有效性, 认知权衡包括隐私控制和隐私风险。用户信息披露决策的认知因素对认知权衡有显著的影响, 进而形成用户披露信息的积极态度和消极态度, 即信任和隐私担忧, 最终信任发挥关键的作用, 连同权衡结果共同影响个人信息披露决策, 即信息披露意愿。

5.2 理论贡献

(1) 应用 CPM 理论的整体框架研究用户披露个人信息决策的过程。已有研究主要采用 CPM 理论的部分准则研究传统网络环境下的隐私问题, 但 PETRONIO^[10] 认为要想理解信息披露的本质, 需要全面考虑 CPM 理论的所有 5 条准则。因此, 本研究基于 CPM 理论整体视角, 构建移动用户个人信息披露决策 3 阶段模型, 从信息披露决策的认知因素到认知权衡, 最终进行披露决策, 揭示了用户个人信息披露决策的形成过程, 并以移动商务为具体情景对该模型进行实证检验。这对移动用户披露个人信息的本质提供了更深层次的理解, 并从理论上丰富了移动商务环境下用户信息披露行为的研究, 进一步拓展了移动环境下隐私问题的研究。

(2) 本研究以移动商务为研究背景, 将信任和隐私担忧视作两种不同的态度(积极态度和消极态度), 同时评估了两者对用户信息披露意愿的相互作用。研究发现, 相对于隐私担忧, 用户对服务商的信任对其个人信息披露意愿发挥着至关重要的作用。结合整个模型的研究结果看, 本研究为移动环境下的隐私悖论现象提供了充分的解释。在当前移动应用更迭迅速的环境下, 隐私悖论可能是用户为顺应潮流迫于无奈的一种外在表现。当移动用户在进行信息披露决策时, 一个信任的环境能为用户提供信心, 促使其感觉个人信息使用情况是安全的。因此, 本研究不但从理论上证明了移动环境下普遍存在的隐私悖论现象, 还进一步对该现象提供了新的见解。

5.3 管理启示

(1) 在移动应用中除设计隐私政策外, 还应重视其他有效的隐私保护措施的开发和设计, 赋予用户对个人信息的披露及其披露后相应的控制力。若移动服务商能为用户提供可选择的明确、详细的隐私披露选项, 会极大地提高用户对个人隐私信息的控制感知, 从而提升他们对移动服务商的信任, 促进用户披露个人信息的意愿。因此, 移动服务商应重视隐私保护措施的设计, 迎合用户的信息控制需求。

(2) 服务商应重视信任的核心作用, 加强企业正面宣传, 提高用户对移动服务商的信任。结合实际情况深入挖掘用户对信息控制的需求, 采取有效的

隐私控制措施,如可告知用户使用差分隐私等^[46]技术处理个人信息,以期营造一种信任氛围,使用户相信移动服务商会妥善地保护、处理其提供的个人信息。

(3) 移动服务商应规范对用户信息的收集行为。当移动服务商不需要或不打算使用某些信息时,应尽量减少对这些信息的收集,并减少未知第三方的参与,以缓解用户被移动服务商监视的感受;还可以保证在不侵犯用户隐私的情况下使用获取的信息,使用户感到安心,缓解其对隐私损失的担忧。

5.4 研究局限和未来展望

(1) 本研究仅以移动商务为情景验证决策模型,后续研究可以针对移动互联网中不同的情景对决策模型进行分析,从而在理论上进一步推进信息隐私和信息披露行为的相关研究,并为企业的管理实践提供更有效的指导。

(2) 本研究的调查对象虽然涉及不同年龄段,但大多数是年轻人样本,虽然年轻人更热衷于使用移动商务应用,相关的调查报告也表明年轻人是使用移动商务应用最大的群体,但是这样的人口结构特征可能影响研究结果的普适性,后续研究将可以在样本构成方面进行改进。

参考文献:

- [1] 谢刚,冯缨,田红云,等. 信息生态视角下移动网络隐私问题及防治措施. *情报理论与实践*, 2015, 38(8): 21-26.
XIE Gang, FENG Ying, TIAN Hongyun, et al. Privacy issues on mobile internet and prevention and control measure under the perspective of information ecology. *Information Studies: Theory & Application*, 2015, 38(8): 21-26.
- [2] WANG T, DUONG T D, CHEN C C. Intention to disclose personal information via mobile applications: a privacy calculus perspective. *International Journal of Information Management*, 2016, 36(4): 531-542.
- [3] CHOI B C F, LAND L. The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage. *Information & Management*, 2016, 53(7): 868-877.
- [4] 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. *情报学报*, 2018, 37(1): 1-13.
LI He, YU Lu, XU Yiming, et al. Research on privacy paradox in social network sites under the perspective of construal level theory. *Journal of the China Society for Scientific and Technical Information*, 2018, 37(1): 1-13.
- [5] BARNES S B. A privacy paradox: social networking in the United States. *First Monday* (Online), 2006, 11(9).
- [6] KOKOLAKIS S. Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. *Computers & Security*, 2017, 64: 122-134.
- [7] SUTANTO J, PALME E, TAN C H, et al. Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users. *MIS Quarterly*, 2013, 37(4): 1141-1164.
- [8] XU H, LUO X, CARROLL J M, et al. The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, 2011, 51(1): 42-52.
- [9] XU H, DINEV T, SMITH H J, et al. Information privacy concerns: linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, 2011, 12(12): 798-824.
- [10] PETRONIO S. *Boundaries of privacy: dialectics of disclosure*. New York: State University of New York Press, 2002: 2-3.
- [11] SHARMA S, CROSSLER R E. Disclosing too much? Situational factors affecting information disclosure in social commerce environment. *Electronic Commerce Research and Applications*, 2014, 13(5): 305-319.
- [12] XU H, GUPTA S, ROSSON M B, et al. Measuring mobile users' concerns for information privacy//*Proceedings of 33rd Annual International Conference on Information Systems*, 2012: 1-16.
- [13] 林家宝,鲁耀斌,卢云帆. 移动商务环境下消费者信任动态演变研究. *管理科学*, 2011, 24(6): 93-103.
LIN Jiabao, LU Yaobin, LU Yunfan. Dynamic evolution of consumer trust in the mobile commerce environment. *Journal of Management Science*, 2011, 24(6): 93-103.
- [14] KEITH M J, BABB J, LOWRY P B, et al. The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal*, 2015, 25(4): 637-667.
- [15] 刘百灵,徐伟,夏惠敏. 应用特征与个体特质双重视角下移动购物持续使用意愿研究. *管理科学*, 2018, 31(2): 59-70.
LIU Bailing, XU Wei, XIA Huimin. A study on the continued use intention of mobile shopping from the perspectives of characteristics for individuals and applications. *Journal of Management Science*, 2018, 31(2): 59-70.
- [16] PETRONIO S. *Balancing the secrets of private disclosures*. London: Lawrence Erlbaum Associates Press, 2000: 37-46.
- [17] CHANG Y H, WONG S F, LEE H S. Understanding perceived privacy: a privacy boundary management model// *Proceedings of the 19th Pacific Asia Conference on Information Systems*, 2015: 1-17.
- [18] PETRONIO S. Communication privacy management theory: what do we know about family privacy regulation?. *Journal of Family Theory & Review*, 2010, 2(3): 175-196.
- [19] PIERCE J L, KOSTOVA T, DIRKS K T. The state of psychological ownership: integrating and extending a century of research. *Review of General Psychology*, 2003, 7(1): 84-107.
- [20] CAUGHLIN J P, GOLISH T D, OLSON L N, et al. Intrafamily secrets in various family configurations: a communication boundary management perspective. *Communication Studies*, 2000, 51(2): 116-134.
- [21] XU H, TEO H H, TAN B C Y, et al. The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of Management Information Systems*, 2009, 26(3): 135-173.
- [22] XU F, MICHAEL K, CHEN X. Factors affecting privacy disclosure on social network sites: an integrated model. *Electronic Commerce Research*, 2013, 13(2): 151-168.
- [23] KENNEDY-LIGHTSEY C D, FRISBY B N. Parental privacy invasion, family communication patterns, and perceived ownership of private information. *Communication Reports*, 2016, 29(2): 75-86.
- [24] MALHOTRA N K, KIM S S, AGARWAL J. Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. *Information Systems Research*, 2004, 15(4): 336-

- 355.
- [25] WU K W, HUANG S Y, YEN D C, et al. The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, 2012, 28(3): 889–897.
- [26] ROMANOSKY S, TELANG R, ACQUISTI A. Do data breach disclosure laws reduce identity theft?. *Journal of Policy Analysis and Management*, 2011, 30(2): 256–286.
- [27] METZGER M J. Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication*, 2007, 12(2): 335–361.
- [28] XU H, TEO H H, TAN B C Y, et al. Research note: effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. *Information Systems Research*, 2012, 23(4): 1342–1363.
- [29] 王小燕. 隐私协议、隐私印章对网络银行顾客信任及使用意向影响研究. *预测*, 2012, 31(1): 14–19.
WANG Xiaoyan. The impact of privacy agreement and privacy seal on trust and intention of online bank customers. *Forecasting*, 2012, 31(1): 14–19.
- [30] BRANDIMARTE L, ACQUISTI A, LOEWENSTEIN G. Mispredicted confidences: privacy and the control paradox. *Social Psychological and Personality Science*, 2013, 4(3): 340–347.
- [31] JOINSON A N, REIPS U D, BUCHANAN T, et al. Privacy, trust, and self-disclosure online. *Human-Computer Interaction*, 2010, 25(1): 1–24.
- [32] 王洪伟, 周曼, 何绍义. 影响个人在线提供隐私信息意愿的实证研究. *系统工程理论与实践*, 2012, 32(10): 2186–2197.
WANG Hongwei, ZHOU Man, HE Shaoyi. Empirical research of individuals' intention to provide privacy information online. *Systems Engineering-Theory & Practice*, 2012, 32(10): 2186–2197.
- [33] YANG Q, PANG C, LIU L, et al. Exploring consumer perceived risk and trust for online payments: an empirical study in China's younger generation. *Computers in Human Behavior*, 2015, 50(C): 9–24.
- [34] YI M Y, YOON J J, DAVIS J M, et al. Untangling the antecedents of initial trust in web-based health information: the roles of argument quality, source expertise, and user perceptions of information quality and risk. *Decision Support Systems*, 2013, 55(1): 284–295.
- [35] 薛可, 何佳, 余明阳. 社会化媒体中隐私悖论的影响因素研究. *当代传播*, 2016(1): 34–38.
XUE Ke, HE Jia, YU Mingyang. Research on the influencing factors of privacy paradox in social media. *Contemporary Communication*, 2016(1): 34–38.
- [36] JIANG Z H, HENG C S, CHOI B C F. Research note: privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research*, 2013, 24(3): 579–595.
- [37] 朱侯. 社交媒体用户隐私关注的心理机制研究. *图书情报知识*, 2016(2): 75–82.
ZHU Hou. Review on psychological mechanism of social media user's privacy concern. *Documentation, Information & Knowledge*, 2016(2): 75–82.
- [38] 邓朝华, 洪紫映. 在线医疗健康服务医患信任影响因素实证研究. *管理科学*, 2017, 30(1): 43–52.
DENG Zhaohua, HONG Ziyi. An empirical study of patient-physician trust impact factors in online healthcare services. *Journal of Management Science*, 2017, 30(1): 43–52.
- [39] LI Y J. A multi-level model of individual information privacy beliefs. *Electronic Commerce Research and Applications*, 2014, 13(1): 32–44.
- [40] BANSAL G, ZAHEDI F M, GEFEN D. Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management*, 2016, 53(1): 1–21.
- [41] 刘百灵, 夏惠敏, 李延晖. 移动购物用户信息披露意愿影响因素的实证研究: 基于公平理论和理性行为理论视角. *情报理论与实践*, 2017, 40(5): 87–93.
LIU Bailing, XIA Huimin, LI Yanhui. An empirical study of factors influencing mobile shopping users' intention to disclose information. *Information Studies: Theory & Application*, 2017, 40(5): 87–93.
- [42] 林家宝, 鲁耀斌, 张金隆. 基于TAM的移动证券消费者信任实证研究. *管理科学*, 2009, 22(5): 61–71.
LIN Jiabao, LU Yaobin, ZHANG Jinlong. An empirical study on consumers' trust of mobile stock based on TAM theory. *Journal of Management Science*, 2009, 22(5): 61–71.
- [43] GU J, XU Y J, XU H, et al. Privacy concerns for mobile app download: an elaboration likelihood model perspective. *Decision Support Systems*, 2017, 94: 19–28.
- [44] DINEV T, HART P J. An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 2006, 17(1): 61–80.
- [45] KOCK N, LYNN G S. Lateral collinearity and misleading results in variance-based SEM: an illustration and recommendations. *Journal of the Association for Information Systems*, 2012, 13(7): 546–580.
- [46] MIDHA V. Impact of consumer empowerment on online trust: an examination across genders. *Decision Support Systems*, 2012, 54(1): 198–205.

Research on Mobile Users' Information Disclosure Decision Process from the Perspective of the Whole CPM Theory

LIU Bailing, SUN Wenjing

School of Information Management, Central China Normal University, Wuhan 430079, China

Abstract: With the development of the mobile Internet and big data, users' data has become the important resources for companies to obtain competitive advantages. But mobile service providers' collection and process of users' data raises users' privacy concerns. The prevalence of privacy paradox phenomena confuses the privacy issues' negative effects on users' information disclosure. Therefore, it is necessary to better understand the essence of users' information disclosure.

Focusing on the cognitive experience of mobile users, this study explores mobile users' information disclosure decisions. ① Based on the whole framework of communication privacy management (CPM) theory, the mobile user's cognitive experience is divided into three stages: cognitive factors stages, cognitive trade-offs stages and disclosure decisions stages; ② focusing on the mobile users' cognitive experiences, from the perspective of privacy paradox, we developed a three stages model of users' personal information disclosure decision under mobile environments; ③ with the mobile commerce environment as a specific situation, and by employing the method of questionnaire survey, we used Smart PLS 3.0 to conduct the structural equations paths analysis with 406 valid data.

The result shows that the cognitive factors of mobile users' information decision-making (perceived ownership, perceived surveillance, disposition to value privacy, and perceived effectiveness of privacy policy) can directly or indirectly impact the cognitive trade-off factors (privacy risk and privacy control) of mobile users' information disclosure decisions. Which then shape their positive and negative attitudes, i.e. trust and privacy concerns in specific context, in which trust plays a critical role, along with the trade-off of risk-control influence users' willingness of personal information disclosure.

This study attempts to apply the whole framework of CPM theory to study the decision-making process of users' disclosure of personal information, deepening the understanding of the process of mobile user's personal information disclosure decision-making for mobile users, and theoretically enriching the research on users' information disclosure behavior in mobile commerce environment. It further confirms the phenomenon of privacy paradox in the mobile commerce environment. At the same time, with mobile commerce environment as the research background, privacy concerns in specific context and trust are regarded as two different attitudes (positive attitude and negative attitude), and the effects of both of them on users' information disclosure intentions are evaluated, providing new insights into the phenomenon of privacy paradox. With the insights, it is of certain guiding significance for mobile service providers and mobile application developers to take targeted measures to obtain more personal information from users.

Keywords: communication privacy management theory; mobile commerce; information disclosure; perceived surveillance; privacy paradox

Received Date: February 3rd, 2018 **Accepted Date:** November 3rd, 2019

Funded Project: Supported by the National Social Science Foundation of China (20BGL283)

Biography: LIU Bailing, doctor in engineering, is an associate professor in the School of Information Management at Central China Normal University. Her research interests cover information systems, privacy protection, and mobile commerce. Her representative paper titled "Achieving a balance between privacy protection and data collection: a field experimental examination of a theory driven information technology solution" was published in the *Information Systems Research* (online, 2021). E-mail: bl_liu@ccnu.edu.cn

SUN Wenjing is a master degree candidate in the School of Information Management at Central China Normal University. Her research interest focuses on information systems. E-mail: 290204688@qq.com □