

在线隐私政策对消费者提供个人信息意愿的影响机制研究 ——信息敏感度的调节作用

梁晓丹 李颖灏 刘芳

(浙江工商大学工商管理学院,杭州 310018)

摘要:基于信号传递理论和沟通隐私管理理论,通过三个2×2的实验设计,分析了在线隐私政策对消费者提供个人信息意愿的具体影响机制,并考察了信息敏感度的调节效应。结果表明:在线隐私政策的告知明确性、权限水平及保护程度对消费者的信息控制感知和隐私风险感知有显著影响;信息敏感度正向调节隐私政策的权限水平、保护程度与感知信息控制之间的关系,负向调节隐私政策的权限水平、保护程度与感知隐私风险之间的关系;感知信息控制和感知隐私风险对消费者提供个人信息意愿有显著影响。

关键词:在线隐私政策;感知信息控制;感知隐私风险;信息敏感度

引言

随着数据挖掘与分析能力的提高以及计算机功能的进步,网站获取消费者信息变得越来越容易。企业可利用专业大数据公司、网页 Cookies 以及 APP 等多种渠道收集到消费者浏览网络、购物、娱乐、出行等工作生活中的大量信息。这些信息具有重要的商业价值,网站通过统计分析能够发现消费者偏好,从而采取更加有针对性的营销策略^[1]。然而,互联网技术为消费者带来便利性的同时也伴随着一定的隐私威胁。由于互联网的开放性和共享性,个人信息一旦被收集,就很容易被快速地传递给第三方^[2]。而且,通过互联网技术,企业还能收集到新形式的个人信息,比如点击流数据或者位置信息,这些信息都超出了传统交易信息的范围^[3]。因此,大多数消费者担心隐私受到侵犯而不愿意在网站上提供个人信息^[4]。

制定网站隐私政策是电商企业主动承诺保护在线消费者个人信息的有效措施,也是吸引消费者注册并参与电子商务交易的关键影响因素之一。已有研究表明,互联网用户在访问网站时已经意识到隐私政策的概念,且越来越多的人开始阅读隐私政策的内容^[5]。隐私政策的信息量^[6]、信息形式^[7]、政策的沟通和传播方法^[8]都会影响人们的感知和行为意向。然而,学者们关于隐私政策影响消费者行为意向的研究结果并不一致。例如,Berendt等^[9]发现隐私政策内容对用户的信息分享行为没有显著影响;Wu等^[10]的研究结论却与之相反,他们通过建立跨文化背景下的隐私-信任-行为意图模型,发现隐私政策的存在有利于个人信息的披露。通过文献的进一步梳理发现,关于隐私政策对用户行为的已有研究主要涉及隐私政策的长度、易读性、完整性等方面^[11],或只是简单比较政策的存在与否对网站的影响^[12],而对隐私政策内容特征缺乏必要的关注。在研究方法上,国内外研究大多倾向于采用内容分析法对在线隐私政策的内容范围进行概括,或是从理论角度讲述网站公布隐私政策的行为^[13]及企业的隐私实践对消费者行为的影响,缺少隐私政策内容对消费者影响机制方面的实证研究^[3]。针对上述研究存在的不足,本文基于信号传递理论和沟通隐私管理理论,以隐私政策的内容特征为切入点,采用情景实验方法,研究隐私政策的告知明确性、权限水平和安全程度对消费者个人信息提供意愿的具体影响机制,并分析信息敏感度(高敏感度信息和低敏感度信息)的调节效应。

收稿日期:2016-07-19

基金项目:国家社会科学基金项目(14BGL151);教育部人文社会科学重点研究基地重大课题(16JJD790055);教育部人文社会科学青年项目(13YJC630253)。

作者简介:梁晓丹,浙江工商大学工商管理学院硕士研究生;李颖灏(通讯作者),浙江工商大学工商管理学院副教授,硕士生导师,博士;刘芳,浙江工商大学工商管理学院硕士研究生。

理论基础与研究假设

1、理论基础

(1)信号传递理论

在线交易的信息流程中消费者处于较为明显的弱势地位,为约束网络企业的信息滥用给消费者带来的信息安全风险,常见做法是政府监管和行业自律。其中,网站公布隐私政策,向用户做出服务开发商如何收集、使用、存储个人信息的承诺声明,并予以践行,是行业自律的重要手段。然而,网站隐私政策的有效性在理论研究中存在着较大争议。Aljukhadar 和 Ouellette^[7]和 Wu 等^[10]都在研究中发现网站隐私政策的存在可以增强消费者对卖家的信任程度,进而提高消费者提供信息的意愿。但 Berendt 等^[9]、Kim 等^[14]学者却对隐私政策的有效性提出质疑,认为消费者并不会对隐私政策内涵给予真正的关注,或隐私政策的繁琐含糊导致消费者难以正确理解并做出决策。对于隐私政策有效性的差异化表现,本文认为信号传递理论提供了一个有益的研究视角。网站公布隐私政策本质上就是一种信号传递机制,而信号传递机制的有效性主要取决于信号本身是否包含足够多的有效信息,且不同类型参与者的传递信号成本存在足够高的差异^[15]。

根据信号传递理论,处于信息弱勢的委托者可以通过某个有成本的行为对产品质量进行甄别。对于网络企业的隐私政策披露而言,主动披露详细周密的隐私政策,会提升企业潜在的法律风险成本。因此,隐私实践水平高的企业更愿意发布详细隐私政策,以此把自身的的信息处理方式传递给消费者,促使消费者做出有利于企业自身的甄别。

(2)沟通隐私管理理论

沟通隐私管理(communication privacy management, CPM)理论,也称为信息边界理论,由 Petronio 于 2002 年提出,它通过检验人如何和为什么解释或隐藏贯穿于各种关系背景中的私人信息,探索了信息披露与隐私之间的关系^[16]。该理论认为,每个人都会构建一个物理或虚拟的信息空间,这个空间即“边界”。一旦隐私边界建立,卷入个体便在共享边界内分配“信任信用点”(trust credit points),这些信任信用点会随着后续双方的行为升高或降低。依据情境或个人条件的不同,当外部实体试图渗入边界时个体就可能感知到“侵犯”,此时,个体揭露或抑制信息的决策受到“边界开放”或“边界关闭”规则的控制。

信息披露既有利益也存在风险,每个人必须平衡需求满足与个人信息披露之间的关系。根据沟通隐私管理理论,人们在信息披露过程中,会通过建立隐私边界来管理和保护自己的隐私,权衡所要披露的信息界限,从而决定是否披露信息。该理论将个人信息与电子商务看做一个沟通的过程,其中,隐私边界是决定人们披露信息的数量、程度和对象的关键因素。因此,当人们感觉无法有效控制个人信息,或者预估的隐私风险很高,即超过了已建立的隐私边界时,就不愿意披露个人信息。沟通隐私管理理论为理解个体决定是否及如何披露个人信息提供了有效的框架,而且该理论已经被广泛应用于员工隐私和消费者隐私的研究中。

2、研究假设

(1)告知明确性与感知信息控制、感知隐私风险

感知信息控制指的是个体认为自己能够决定个人信息在网站上被公布到何种程度的能力^[17]。在线隐私政策作为一种行业自律形式,它明确告知了消费者关于企业收集、使用、保护个人信息的方法。Luzak^[18]认为,如果网站在隐私政策中完全告知消费者 Cookies 的使用,消费者会更加愿意个人信息被使用和获取。Xu 等^[19]证明了隐私保护方法会通过信息控制降低用户的隐私担忧。Stutzman 等^[20]表明,网站对用户隐私功能使用的设置、隐私信息利用的透明度及信息传递的自由性都会提升用户对信息的掌控能力。感知隐私风险被定义为个体对在线披露个人信息所遭受的负面结果的期望感知^[17]。借助效用最大化理论,Awad 和 Krishnan^[1]证明了信息透明的重要性与感知风险之间存在显著关系。也就是说,那些希望信息处理更透明的消费者更不愿意被识别。Milne 和 Culnan^[21]认为,在线隐私政策提供了关于商家如何处理消费者信息的说明,因而会降低消费者在线披露个人信息的感知风险。基于此,本文提出如下假设:

H1a: 隐私政策对个人信息的处理方式告知越明确,消费者感知到的信息控制能力越强;

H1b: 隐私政策对个人信息的处理方式告知越明确,消费者感知到的隐私风险越低。

(2) 权限水平与感知信息控制、感知隐私风险

消费者认为,商家未经允许就与第三方共享其个人信息的行为是不可接受的^[4]。而且,当人们同意公司收集个人信息或是自己被给予“退出”的选项时,他们的忧虑会降低^[22]。在互联网环境下,消费者如果想要完成在线交易,就必须点击企业网站的“同意”选项,这种行为必然会提升消费者的隐私忧虑。同时,在个人信息流转环节,企业在整个信息处理过程中均占上风,在线消费者同电商企业之间在信息控制与信息流转的参与方面存在严重的力量失衡。而有效的隐私政策允许消费者自己做出选择,即是否愿意将个人信息用于初始交易以外的目的^[23]或者与第三方共享^[24],同时为消费者提供了查看、修改、删除个人信息的权利,这能够增强消费者对个人信息使用的控制感知。Jin 等^[8]采用实验调查法,发现在线社交网站中隐私政策的权限水平会通过用户隐私风险感知影响个人信息披露意愿。基于此,本文提出如下假设:

H2a: 隐私政策授予用户的权限水平越高,消费者感知到的信息控制能力越强;

H2b: 隐私政策授予用户的权限水平越高,消费者感知到的隐私风险越低。

(3) 保护程度与感知信息控制、感知隐私风险

在绝大多数电子商务中,消费者要想体验网络交易带来的个性化和便利性,就必须提供个人信息(如姓名、地址、信用卡号码等)。除此之外,网站还可利用 Cookies 跟踪消费者的爱好和使用记录,或者使用 ActiveX、Java 等获取个人的信用数据。然而,由于互联网既无边界也缺乏监管,再加上网络传播的迅捷性和广泛性,个人信息一旦在网上披露,瞬间可被全世界知晓,给当事人带来意料不到的严重后果。因此,当个人信息缺乏保护时,大多数在线消费者不愿意提供个人信息。Li 等^[25]研究表明,如果在线供应商能够如约保护消费者个人信息,消费者对其个人信息的披露及后续使用将会感知到更明显的控制。从理论上讲,只有当网站的隐私政策表明公司会保护消费者隐私时,消费者的风险感知才会降低。Culnan 和 Armstrong^[26]发现,当企业采用适当的措施来保护个人隐私时,消费者会愿意提供个人信息,并允许企业将个人信息用于创建商业用途的客户资料。基于此,本文提出如下假设:

H3a: 隐私政策对个人信息的保护程度越高,消费者感知到的信息控制能力越强;

H3b: 隐私政策对个人信息的保护程度越高,消费者感知到的隐私风险越低。

(4) 信息敏感度的调节作用

Malhotra 等^[12]将信息的风险属性定义为“信息敏感度”。人们普遍认为财务信息、医疗信息和个人可识别信息比生活习惯、购买行为和人口统计信息更加敏感,因而更愿意披露人口统计信息和生活方式信息^[27]。根据 Malhotra 等的研究,敏感度高的信息会对消费者的态度和披露个人信息意愿产生更加负面的影响^[12]。也就是说,在其他因素都相同的情况下,当消费者披露敏感度高的信息时也会感知到更高的风险水平^[25]。Sheehan 和 Hoy^[28]等研究表明,消费者对隐私敏感度的感知会影响对隐私政策的感知。根据沟通隐私管理理论,消费者披露信息的决定受到“边界关闭”或“边界开放”规则的控制^[16]。在面对同样的隐私政策情境下,当网站需要提供的信息的敏感度较低时,消费者对隐私政策的感知受信息类型的影响不大,此时“信息边界”打开,并愿意提供个人信息;而当网站需要提供的信息的敏感度较高时,消费者会更加关注组织的在线隐私政策,同时表现出更强的识别能力、更低的信任程度^[29]。在这种情况下,消费者会感觉对信息的控制能力减弱,并认为可能会产生更严重的潜在后果。因此,即便消费者理解信息共享的必要性,他们也不愿意完全披露所要求的信息^[30]。许多学者一致认为,用户对隐私威胁的反应取决于被请求的信息类型^[12,31]。基于此,本文提出如下假设:

H4a: 当要求提供的信息敏感度越高时,隐私政策对个人信息处理方式告知的明确性对消费者信息控制感知的正向影响越强;

H4b: 当要求提供的信息敏感度越高时,隐私政策对个人信息处理方式告知的明确性对消费者隐私风险感知的负向影响越弱;

H4c: 当要求提供的信息敏感度越高时,隐私政策赋予消费者的权限水平对其信息控制感知的正向影响越强;

H4d: 当要求提供的信息敏感度越高时,隐私政策赋予消费者的权限水平对其隐私风险感知的负向影响越弱;

H4e:当要求提供的信息敏感度越高时,隐私政策的保护程度对消费者信息控制感知的正向影响越强;

H4f:当要求提供的信息敏感度越高时,隐私政策的保护程度对消费者隐私风险感知的负向影响越弱。

(5)感知信息控制、感知隐私风险与个人信息提供意愿

研究表明,消费者缺乏对其个人信息的控制是与隐私相关的主要忧虑之一^[22]。Song 等^[32]认为,相对于获得报酬而言,用户更愿意获取对个人信息的控制权。因此,对电商企业而言,解决用户隐私关注及建立信任的最好方法是允许用户控制个人信息^[33]。Bartsch 和 Dienlin^[34]通过调查社交网站发现,信息控制对社交媒体用户判断是否披露信息非常重要。Brandimarte 等^[35]发现,当用户的信息控制感知增强时,被试更愿意披露个人信息(包括敏感信息)。感知隐私风险对个人信息提供意愿的负向影响在互联网环境中也已经得到了验证^[36]。Youn^[37]在调查青少年的隐私保护问题时,发现青少年对信息披露的感知风险水平越高,越不愿意提供个人信息。Norberg 等^[38]研究表明,信息披露的风险感知会对消费者向营销人员提供个人信息的意愿产生负向影响。同样,Hajli 和 Lin^[39]认为,在社交网站中隐私风险感知对用户的个人信息披露态度存在显著影响。基于此,本文提出如下假设:

H5:消费者的信息控制感知正向影响其提供个人信息的意愿。

H6:消费者的隐私风险感知负向影响其提供个人信息的意愿。

基于以上假设,本文提出的研究模型如图 1 所示。

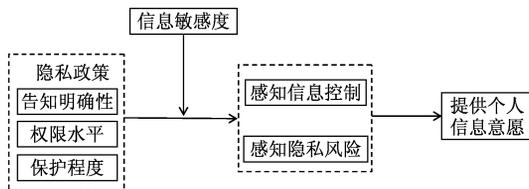


图 1 本文的研究模型

研究方法

1、前测

本研究实验材料的前测主要针对在线隐私政策内容特征和信息敏感度展开。

首先是隐私政策内容特征变量的量表构建。根据美国联邦贸易委员会(FTC)的公平信息实践原则^[40]和 Wu 等^[10]关于隐私政策测量的研究成果,对卓越亚马逊、当当等购书网站以及天猫、淘宝、京东等购物网站的隐私政策进行重点分析,在对 Alexa 排名前 100 中文网站中购物网站的隐私政策进行详细调查的基础上,对公开呈现隐私政策的 67 家网站的隐私政策内容进行文本分析。通过文本分析和焦点小组访谈,构建包括告知明确性、权限水平和保护程度三个维度的隐私政策内容特征量表。信效度检验结果表明,隐私政策内容特征变量的 KMO 值为 0.731,克朗巴哈 α 值均大于 0.753,所有因子载荷值均介于 0.678 至 0.887 之间,且全部测量指标的因子载荷 t 值都达到 $p < 0.001$ 的统计显著水平;组合信度 CR 值均大于 0.80,大于 0.60 的可接受水平;平均提取方差 AVE 均大于 0.50,对角线上 AVE 的平方根均大于相应行列中的相关系数。三因素模型拟合指数为 $\chi^2 = 41.616$, $\chi^2/df = 1.300$, RMSEA = 0.04, NFI = 0.948, CFI = 0.987, GFI = 0.960, AGFI = 0.931, 表明模型拟合良好。由此可见,本研究构建的在线隐私政策内容特征量表具有较好的信效度。

然后,针对在线隐私政策的告知明确性、权限水平和保护程度三个维度,根据隐私政策中收集信息类型、收集途径、收集目的、信息的用途、Cookies 的使用、信息披露条件解释的详细程度等将隐私政策划分为告知明确的隐私政策和告知不明确的隐私政策;根据消费者是否可以选接收推送的信息、是否可以拒绝个人信息的共享、是否可以查看/修改/删除个人信息等将隐私政策划分为用户权限水平高的隐私政策和用户权限水平低的隐私政策;同时根据网站是否采取各种措施保护消费者信息的安全以及是否提供申诉的途径,将在线隐私政策区分为对个人信息保护程度高的隐私政策和保护程度低的隐私政策。利用上述素材的不同组合,我们形成了 6 篇不同内容的隐私政策。然后,我们请 40 位在校大学生(23 名女生,17 名男生)对每一篇隐私政策就告知明确性、权限水平和保护程度进行李克特 7 级评分。评分结果显示,告知明确(5.02)与告知不明确(3.31)、权限水平高(5.12)和低(4.08)、保护程度高(4.82)和低(3.98)的隐私政策在得分上有显著差异。

为了选取合适的高敏感度信息和低敏感度信息进行实验,本研究参考 Yang 和 Wang^[41]、朱慧等^[42]和李睿等^[43]的研究成果,邀请 10 名大学生在李克特 7 级量表上对各项购物情境中常被要求提供的信息,进行信息敏感度的心理反应值评定,并进行信息类型的划分。最终选取性别、民族、身高、体重、个人兴趣爱好、个人购物偏好等 8 项人口统计信息为低敏感度信息,上述人口统计信息与手机号码、身份证号、银行卡号以及支付宝账号等身份识别和财务信息组成的 16 项信息集合为高敏感度信息。然后邀请 30 位在校大学生(17 位女生,13 位男生)对两种信息集合的敏感度进行评价,独立样本 t 检验显示高敏感度信息的敏感度($M=5.27$)显著高于低敏感度信息($M=2.63$), $t=12.41$ 。

2、实验设计

本研究设计了三个情境实验来对前述假设进行检验。实验一采用 2(告知明确性:告知不明确/告知明确) \times 2(信息敏感度:低/高)的组间设计,检验告知明确性、信息敏感度对消费者提供信息意愿的影响及其交互效应;实验二采用 2(权限水平:低/高) \times 2(信息敏感度:低/高)的组间设计,检验权限水平、信息敏感度对消费者提供信息意愿的影响及其交互效应;实验三采用 2(保护程度:低/高) \times 2(信息敏感度:低/高)的组间设计,检验保护程度、信息敏感度对消费者提供信息意愿的影响及其交互效应。本研究设计了 6 种不同内容的隐私政策,共 12 种问卷类型,随机发放并要求被试填写相应的问卷。

问卷共由七部分组成。第一部分介绍购书网站;第二部分对 6 种隐私政策的其中一种进行展示;第三部分为网站要求消费者提供的信息项目;第四部分由被试填写对各种信息的提供意愿;第五部分分别对在线隐私政策的三个维度(告知明确性、权限水平、保护程度)进行操控测量;第六部分测量被试的信息控制感知和隐私风险感知;第七部分是被试的个人基本信息调查。通过预实验及问项净化后形成李克特 7 点量表和调查问卷。

3、数据收集

本研究以在校大学生为调查对象,并以图书网站作为网站的研究类型。根据中国互联网络信息中心(CNNIC)发布的第 38 次《中国互联网络发展状况统计报告》和《2015 年中国网络购物市场研究报告》,网民结构中中学生群体规模最大,学生群体占比为 25.2%;网络购物中书籍音像制品类占比 51%,位居网购品类的第三位。另据中国新闻出版研究院《第 12 次全国国民阅读调查报告(2015)》,大学生的学习需求更加多元和广泛,通过网络购书来满足学习兴趣和需求,是教育类、自我发展类书籍的主要消费群体。基于此,本文选择了图书网站作为研究的网站类型。同时,为了消除大学生受试受特定网站声誉或熟悉度带来的干扰,本文综合了亚马逊(中国)、当当网以及包含图书品类经营项目的京东等购物网站的特征,构建了一个虚拟的购书网站,并主要参考上述网站以及 Alexa 排名前 100 的中文网站的隐私政策声明,形成了实验材料。

我们采用纸质问卷和问卷星两种方式在大学生群体中发放问卷,采用随机抽取情境,自愿填答的方式,被试在阅读隐私政策之后如实填写问卷。共发放问卷 720 份,回收 680 份,其中有效问卷 600 份。通过问卷星发放问卷 100 份,纸质问卷 620 份,其中问卷星回收问卷 67 份,有效问卷 46 份;纸质问卷回收 613 份,有效问卷 554 份。有效被试中,男性占 38.5%,女性占 61.5%。年龄 18-24 岁的被试 472 名,占 78.67%,25-30 岁被试 125 名,占 20.83%,31-35 岁被试 3 名,占 0.5%。

4、变量测量

个人信息提供意愿的测量,主要结合了 Malhotra 等^[12]和王洪伟等^[44]的量表,共有 3 个问项;感知信息控制的测量,主要采用了 Dinev 等^[17]的量表,共有 5 个问项;感知隐私风险参考了 Dinev 等^[17]和 Malhotra 等^[12]的量表,最终形成 3 个问项。上述变量测量均采取李克特 7 级评分,从 1(非常不同意)到 7(非常同意),供被试作答。

5、信度、效度分析

对于信度而言,对中介变量“感知信息控制”和“感知隐私风险”的信度分析表明,Cronbach's α 系数分别为 0.869 和 0.868;对因变量“个人信息提供意愿”量表的信度分析表明,此量表 Cronbach's α 系数为 0.806。

从内容效度来看,上述变量测量语句源自于已有研究文献,并与相关专家进行了深入探讨,具有一定的内容效度。

数据分析

1、实验一数据分析

(1)隐私政策告知明确性的操控检验。对实验一获得的数据进行独立样本 t 检验,结果显示:告知不明确组被试的认可度均值为 3.87,告知明确组被试的认可度均值 4.66;且两组之间差异显著($t = -5.187, p < 0.001$)。由此可见,隐私政策的告知明确性变量得到了成功操控。

(2)实验一相关假设检验。根据实验一所获数据,以感知信息控制和感知隐私风险作为结果变量,进行 2(告知明确性:不明确/明确) \times 2(信息敏感度:低/高)双因素 ANOVA 分析。结果显示(见表 1、表 2),告知明确性对感知信息控制($F = 15.696, p = 0.000 < 0.001$)和感知隐私风险($F = 4.648, p = 0.032 < 0.05$)的主效应都显著,即当网站隐私政策对个人信息处理方式告知越明确时,消费者感知到的信息控制能力越强,隐私风险感知越小,H1a、H1b 得到有效验证;告知明确性与信息敏感度对感知信息控制和感知隐私风险的交互影响作用都不显著,H4a、H4b 不成立;与此同时,感知信息控制($F = 4.502, p = 0.035 < 0.05$)对消费者提供个人信息意愿有显著正向影响;感知隐私风险($F = 5.659, p = 0.018 < 0.05$)对消费者提供个人信息意愿存在显著负向影响,假设 H5、H6 得到有效验证。

表 1 告知明确性与信息敏感度对感知信息控制的交互影响作用检验

自变量	df	均方	F	p
告知明确性	1	21.780	15.696***	0.000
信息敏感度	1	7.373	5.313*	0.022
告知明确性 * 信息敏感度	1	1.479	1.066	0.303
误差	196	1.388		

表 2 告知明确性与信息敏感度对感知隐私风险的交互影响作用检验

自变量	df	均方	F	p
告知明确性	1	5.120	4.648*	0.032
信息敏感度	1	1.742	1.582	0.210
告知明确性 * 信息敏感度	1	0.980	0.890	0.347
误差	196	1.101		

2、实验二数据分析

(1)隐私政策权限水平的操控检验。对实验二获得的数据进行独立样本 t 检验,结果显示:权限水平低组被试的认可度均值为 4.10,权限水平高组被试的认可度均值 4.93;且两组之间差异显著($t = -4.193, p < 0.001$)。由此可见,隐私政策的权限水平变量操控成功。

(2)实验二相关假设检验。根据实验二所获数据,以感知信息控制和感知隐私风险作为结果变量,进行 2(权限水平:低/高) \times 2(信息敏感度:低/高)双因素 ANOVA 分析。结果显示(见表 3、表 4),权限水平对感知信息控制($F = 20.053, p = 0.000 < 0.001$)和感知隐私风险($F = 17.359, p = 0.000 < 0.001$)的主效应都显著,即当网站隐私政策的权限水平越高时,消费者感知到的信息控制能力越强,隐私风险感知越小,H2a、H2b 得到有效验证;与此同时,感知信息控制($F = 5.749, p = 0.017 < 0.05$)对消费者提供个人信息意愿有显著正向影响;感知隐私风险($F = 12.869, p = 0.000 < 0.001$)对消费者提供个人信息意愿存在显著负向影响,假设 H5、H6 得到有效验证。

由表 3 可知,隐私政策的权限水平与信息敏感度对感知信息控制的交互效应显著($F = 4.905, p = 0.028 < 0.05$),假设 H4c 得到有效验证。具体来说(见图 2),当网站所要求信息的敏感度较低时,隐私政策的权限水平对消费者的信息控制感知不存在显著差异($M_{\text{水平高}} = 3.856$ vs. $M_{\text{水平低}} = 3.484; F = 2.561, p = 0.111 > 0.05$),当网站所要求信息的敏感度较高时,隐私政策的权限水平对消费者的信息控制感知存在显著差异($M_{\text{水平高}} = 3.732$ vs. $M_{\text{水平低}} = 2.632; F = 22.397, p = 0.000 < 0.001$);由表 4 可知,隐私政策的权限水平与信息敏感度对感知隐私风险的交互效应也显著($F = 4.211, p = 0.041 < 0.05$),假设 H4d 得到有效验证。具体来说(见图 3),当网站所要求信息的敏感度较低时,隐私政策的权限水平对消费者的隐私风险感知存在显著差异($M_{\text{水平高}} = 4.32$ vs. $M_{\text{水平低}} = 5.32; F = 19.335, p = 0.000 < 0.001$),当网站所要求信息的敏感

度较高时,隐私政策的权限水平对消费者的隐私风险感知不存在显著差异($M_{\text{水平高}} = 5.16$ vs. $M_{\text{水平低}} = 5.50$; $F = 2.235, p = 0.137 > 0.05$)。

表 3 权限水平与信息敏感度对感知信息控制的交互影响作用检验

自变量	df	均方	F	p
权限水平	1	27.085	20.053***	0.000
信息敏感度	1	11.907	8.816**	0.003
权限水平 * 信息敏感度	1	6.625	4.905*	0.028
误差	196	1.351		

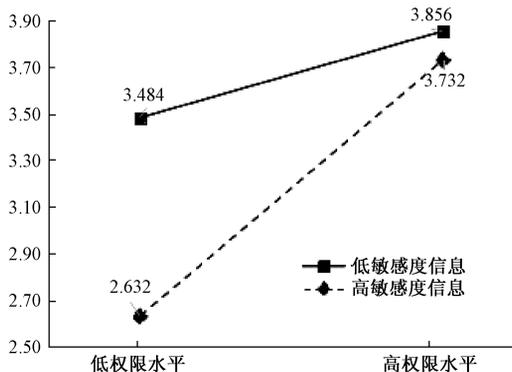


图 2 权限水平与信息敏感度对感知信息控制的交互作用

表 4 权限水平与信息敏感度对感知隐私风险的交互影响作用检验

自变量	df	均方	F	p
权限水平	1	22.445	17.359***	0.000
信息敏感度	1	13.005	10.058**	0.002
权限水平 * 信息敏感度	1	5.445	4.211*	0.041
误差	196	1.293		

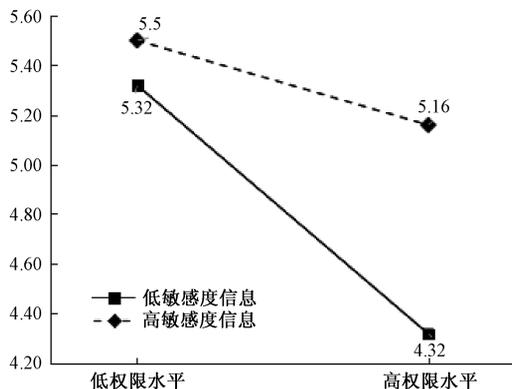


图 3 权限水平与信息敏感度对感知隐私风险的交互作用

3、实验三数据分析

(1) 隐私政策保护程度的操控检验。对实验三获得的数据进行独立样本 t 检验,结果显示:保护程度低组被试的认可度均值为 4.05,保护程度高组被试的认可度均值 4.70;且两组之间差异显著($t = -3.717, p < 0.001$)。由此可见,隐私政策的保护程度变量操控成功。

(2) 实验三相关假设检验。根据实验三所获数据,以感知信息控制和感知隐私风险作为结果变量,进行 2(保护程度:高/低)×2(信息敏感度:高/低)双因素 ANOVA 分析。结果显示(见表 5、表 6),保护程度对感知信息控制($F = 20.536, p = 0.000 < 0.001$)和感知隐私风险($F = 25.662, p = 0.000 < 0.001$)的主效应都显著,即当网站隐私政策的保护程度越高时,消费者感知到的信息控制越强,隐私风险越低,H3a、H3b 得到有效验证;与此同时,感知信息控制($F = 19.013, p = 0.000 < 0.001$)对消费者的个人信息提供意愿有显著正向影响;感知隐私风险($F = 6.205, p = 0.014 < 0.05$)对消费者的个人信息提供意愿存在显著负向影响,假设 H5、H6 再次得到

有效验证。

由表 5 可知,网站隐私政策的保护程度与信息敏感度对感知信息控制的交互效应显著($F = 4.697, p = 0.031 < 0.05$),假设 H4e 得到有效验证。具体来说(见图 4),当网站所要求信息的敏感度较低时,网站隐私政策的保护程度对消费者的信息控制感知存在显著差异($M_{\text{程度高}} = 4.204$ vs. $M_{\text{程度低}} = 3.116; F = 22.438, p = 0.000 < 0.001$),当网站所要求信息的敏感度较高时,网站隐私政策的保护程度对消费者的信息控制感知没有显著差异($M_{\text{程度高}} = 3.380$ vs. $M_{\text{程度低}} = 2.996; F = 2.795, p = 0.096 > 0.05$);由表 6 可知,隐私政策的保护程度与信息敏感度对感知隐私风险的交互效应也显著($F = 5.357, p = 0.022 < 0.05$),假设 H4f 得到有效验证。具体来说(见图 5),当网站所要求信息的敏感度较低时,网站隐私政策的保护程度对消费者的隐私风险感知没有显著差异($M_{\text{程度高}} = 4.62$ vs. $M_{\text{程度低}} = 5.04; F = 3.785, p = 0.053 > 0.05$),当网站所要求信息的敏感度较高时,网站隐私政策的保护程度对消费者的隐私风险感知存在显著差异($M_{\text{程度高}} = 4.64$ vs. $M_{\text{程度低}} = 5.767; F = 27.234, p = 0.000 < 0.001$)。

表 5 保护程度与信息敏感度对感知信息控制的交互影响作用检验

自变量	df	均方	F	p
保护程度	1	27.058	20.536***	0.000
信息敏感度	1	11.139	8.446**	0.004
保护程度 * 信息敏感度	1	6.195	4.697*	0.031
误差	196	1.319		

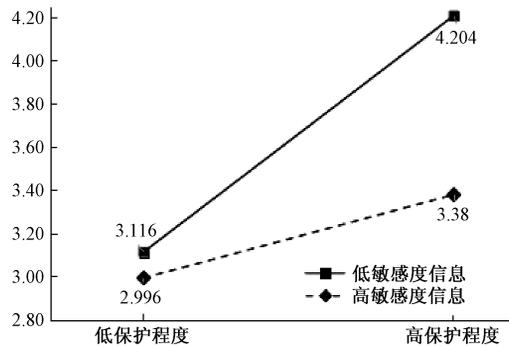


图 4 保护程度与信息敏感度对感知信息控制的交互作用

表 6 保护程度与信息敏感度对感知隐私风险的交互影响作用检验

自变量	df	均方	F	p
保护程度	1	29.902	25.662***	0.000
信息敏感度	1	6.969	5.981*	0.015
保护程度 * 信息敏感度	1	6.242	5.357*	0.022
误差	196	1.165		

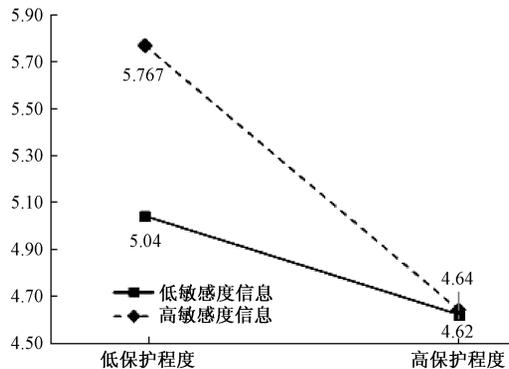


图 5 保护程度与信息敏感度对感知隐私风险的交互作用

结论与讨论

1、研究结论

本研究关于在线隐私政策对消费者提供个人信息意愿的影响机制进行了初步研究,同时考察了感知隐私风险、感知信息控制等心理机制及信息敏感度在整个过程中所起的作用。首先,在线隐私政策的内容特征对消费者感知到的信息控制和隐私风险存在显著影响。具体来说,在线隐私政策明确告知对个人信息处理方式,赋予消费者对自己信息的更多处理权限,或采取更有力保护措施以防止各类信息的丢失和滥用,能够使消费者的信息控制感知显著提高,隐私风险感知显著降低,进而提高个人信息的提供意愿。同时研究也发现,信息敏感度在网站隐私政策内容特征对消费者信息控制感知和隐私风险感知的影响中存在部分调节作用,具体而言,信息敏感度高低改变了在线隐私政策的权限水平和控制程度两个内容特征对消费者信息控制感知和隐私风险感知的影响大小,即信息敏感度正向调节隐私政策的权限水平、保护程度与感知信息控制之间的关系,负向调节隐私政策的权限水平、保护程度与感知隐私风险之间的关系,而信息敏感度对告知明确性与消费者心理感知作用关系的调节作用不显著。其原因可能是当在线隐私政策对个人信息的处理方式告知越明确、越详细时,消费者越能够准确地评估电子商务企业做出不当行为的可能性,并根据在线隐私政策内容进行理性、客观的判断,因而无论网站需要低敏感度信息还是高敏感度信息,消费者都不会轻易改变已形成的心理感知。

2、理论贡献

本研究是对 Belanger 和 Crossler^[3] 学者呼吁大数据背景下开展更多在线隐私政策内在作用机制研究的积极回应,通过在线隐私政策对消费者提供个人信息意愿影响机制的组合设计,初步打开了在线隐私政策内在效用机制的“黑箱”。此外,研究采用信号传递理论和 CPM 理论,针对过去探讨网站隐私政策效果缺少对心理机制影响的研究,选择感知信息控制和感知隐私风险两个关键心理机制,并探讨了信息敏感度高低对在线隐私政策影响消费者心理感知及信息提供意愿中存在的调节作用,加深了对网站隐私政策作用机制的认知,并在一定程度上充实了现有网站隐私政策作用机制的研究。

3、管理启示

首先,网络企业不仅要主动公布自己的隐私政策,还应高度重视在线隐私政策在告知明确性、权限水平和保护程度等方面的内容特征设计。在线隐私政策需要以专业化、规范化的形式向消费者传达企业实际的隐私实践,使消费者对企业网站对个人信息的收集、使用、共享过程更加清楚;同时,企业在使用信息之前要尽可能地获取消费者明确许可,并使消费者有权查看、修改、删除个人信息;另外,企业还要从技术方面和管理方面加强对消费者个人信息的保护程度。

其次,感知隐私风险和感知信息控制是解释消费者个人信息提供意愿的重要变量,不同内容特征的隐私政策带给消费者的信息控制感知和隐私风险感知不同,企业网站应从消费者角度出发,制定出明确、完善的在线隐私政策,同时通过更多的解释、信息披露和针对性沟通策略,以提高消费者信息控制感知和降低隐私风险感知。

第三,在线隐私政策的权限水平和隐私保护程度对消费者心理感知的影响,在低敏感度信息和高敏感度信息之间存在较大的差异。因此,网站应重点保护高敏感度信息的隐私安全,当需要收集这类信息时,在线隐私政策要特别突出其给予消费者的权利,例如在获得用户明确表示同意之前,不主动获取用户的高敏感信息;同时,加强为保护消费者个人信息而对制度修订、技术手段等各种措施的运用,使消费者形成客观、理性的判断和认知,从而降低消费者做出消极评估结果的可能性。

3、研究局限及展望

本研究得出的结论具有一定的实践意义,同时还存在其他一些值得深入探讨的问题。首先,本研究选择网站隐私政策的内容特征作为前因变量并进行分析,但网站隐私政策仍存在许多需要进一步挖掘的属性,如在线隐私政策的呈现位置与呈现方式,以及隐私政策的执行程序 and 效果等。因此,后续可以从网站隐私政策的其他属性出发进一步深入研究,以持续完善已有的研究成果;其次,消费者隐私意识的确在不断提升,但仍存在较多消费者没有给予在线隐私政策必要的关注,这可能与消费者隐私安全知识、隐私侵犯经历亦或个体认知思维方式有一定的关系,以后或可以从消费者个人特质等角度对此展开研究。最后,本研究被试为在校

大学生,是考虑到大学生在互联网行为中具有代表性,但本研究的实验对象范围仍相对较狭窄,研究结论的普适性在一定程度上受到了影响。未来研究中,有必要针对更大范围和更多类型的互联网用户样本来验证和扩展该研究的结果。

参考文献:

- [1] Awad N. F., Krishnan M. S. The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization[J]. *MIS Quarterly*, 2006,30(1):13-28
- [2] Spiekermann S., Acquisti A., Böhme R., et al. The Challenges of Personal Data Markets and Privacy[J]. *Electronic Markets*, 2015,25(2):161-167
- [3] Belanger F., Crossler R. E. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems[J]. *MIS Quarterly*, 2011,35(4):1017-1042
- [4] Caudill E. M., Murphy P. E. Consumer Online Privacy: Legal and Ethical Issues[J]. *Journal of Public Policy & Marketing*, 2013,19(1):7-19
- [5] Baek Y. M., Kim E., Bae Y. My Privacy Is Okay, but Theirs Is Endangered: Why Comparative Optimism Matters in Online Privacy Concerns[J]. *Computers in Human Behavior*, 2014,31(2):48-56
- [6] Capistrano E. P. S., Chen J. V. Information Privacy Policies: The Effects of Policy Characteristics and Online Experience[J]. *Computer Standards & Interfaces*, 2015,42:24-31
- [7] Aljukhadar M., Ouellette S. S. D. Can the Media Richness of a Privacy Disclosure Enhance Outcome? A Multifaceted View of Trust in Rich Media Environments[J]. *International Journal of Electronic Commerce*, 2010,14(4):103-126
- [8] Jin G., Widjaja T., Buxmann P. Handle with Care: How Online Social Network Providers' Privacy Policies Impact Users' Information Sharing Behavior[J]. *Journal of Strategic Information Systems*, 2015,24(1):33-43
- [9] Berendt B., Ntwer O., Spiekermann S. Privacy in E-Commerce: Stated Preferences vs. Actual Behavior[J]. *Communications of the ACM*, 2005,48(4):101-106
- [10] Wu K. W., Huang S. Y., Yen D. C. et al. The Effect of Online Privacy Policy on Consumer Privacy Concern and Trust[J]. *Computers in Human Behavior*, 2012,28(3):889-897
- [11] Ermakova T., Krasnova H., Fabian B. Exploring the Impact of Readability of Privacy Policies on Users' Trust[C]. *The 24th European Conference on Information Systems*, 2016
- [12] Malhotra N. K., Kim S. S., Agarwal J. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model[J]. *Information Systems Research*, 2004,15(4):336-355
- [13] Zhao L., Lu Y., Gupta S. Disclosure Intention of Location-Related Information in Location-Based Social Network Services[J]. *International Journal of Electronic Commerce*, 2014,16(4):53-90
- [14] Kim D. J., Steinfield C., Lai Y. J. Revisiting the Role of Web Assurance Seals in Business-to-Consumer Electronic Commerce[J]. *Decision Support System*, 2008,44(4):1000-1015
- [15] 王宇,魏守华. 网络交易市场中第三方标记的有效性研究——基于信号传递理论的一个解释[J]. *管理评论*, 2016,28(9):51-60
- [16] Petronio S. *Boundaries of Privacy: Dialectics of Disclosure*[M]. New York: State University of New York Press, 2002
- [17] Dinev T., Xu H., Smith J. H. et al. Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts[J]. *European Journal of Information Systems*, 2013,22(3):295-316
- [18] Luzak J. A. Privacy Notice for Dummies? Towards European Guidelines on How to Give "Clear and Comprehensive Information" on the Cookies 'Use in Order to Protect the Internet Users' Right to Online Privacy[J]. *Journal of Consumer Policy*, 2014,163(4):251-257
- [19] 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[J]. *Journal of Management Information Systems*, 2010,26(3):135-174
- [20] Stutzman F., Gross R., Acquisti A. Silent Listeners: The Evolution of Privacy and Disclosure on Facebook[J]. *Journal of Privacy and Confidentiality*, 2012,4(2):7-41
- [21] Milne G. R., Culnan M. J. Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy

- Notices[J]. *Journal of Interactive Marketing*, 2004,18(3):15-29
- [22] Nowak G. J., Phelps J. Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When “Privacy” Matters[J]. *Journal of Direct Marketing*, 1995,9(3):46-60
- [23] Foxman E. R., Kilcoyne P. Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues[J]. *Journal of Public Policy & Marketing*, 1993,12(1):106-119
- [24] Nowak G. J., Phelps J. Understanding Privacy Concerns. An Assessment of Consumers’ Information-Related Knowledge and Beliefs[J]. *Journal of Direct Marketing*, 1992,6(4):28-39
- [25] Li H., Sarathy R., Xu H. The Role of Affect and Cognition on Online Consumers’ Decision to Disclose Personal Information to Unfamiliar Online Vendors[J]. *Decision Support Systems*, 2011,51(3):434-445
- [26] Culnan M. J., Armstrong P. K. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation[J]. *Organization Science*, 1999,10(1):104-115
- [27] Dinev T., Hart P. Privacy Concerns and Levels of Information Exchange: An Empirical Investigation of Intended E-Services Use [J]. *E-Service Journal*, 2007,4(3):25-61
- [28] Sheehan K. B., Hoy M. G. Dimensions of Privacy Concern Among Online Consumers[J]. *Journal of Public Policy & Marketing*, 2013,19(1):62-73
- [29] Rohm A. J., Milne G. R. Just What the Doctor Ordered: The Role of Information Sensitivity and Trust in Reducing Medical Information Privacy Concern[J]. *Journal of Business Research*, 2004,57(9):1000-1011
- [30] Wakefield R. The Influence of User Affect in Online Information Disclosure[J]. *The Journal of Strategic Information Systems*, 2013,22(2):157-174
- [31] Phelps J., Nowak G., Ferrell E. Privacy Concerns and Consumer Willingness to Provide Personal Information[J]. *Journal of Public Policy & Marketing*, 2013,19(1):27-41
- [32] 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):1-13
- [33] Chen K., Rea A. L. Protecting Personal Information Online: A Survey of User Privacy Concerns and Control Techniques[J]. *Journal of Computer Information Systems*, 2004,44(4):85-92
- [34] Bartsch M., Dienlin T. Control Your Facebook: An Analysis of Online Privacy Literacy[J]. *Computers in Human Behavior*, 2016,56:147-154
- [35] Brandimarte L., Acquisti A., Loewenstein G. Misplaced Confidences Privacy and the Control Paradox[J]. *Social Psychological & Personality Science*, 2013,4(3):340-347
- [36] Dinev T., Hart P. An Extended Privacy Calculus Model for E-Commerce Transactions[J]. *Information Systems Research*, 2006,17(1):61-80
- [37] Youn S. Teenagers’ Perceptions of Online Privacy and Coping Behaviors: A Risk-Benefit Appraisal Approach[J]. *Journal of Broadcasting & Electronic Media*, 2005,49(1):86-110
- [38] Norberg P. A., Horne D. R., Horne D. A. et al. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors[J]. *Journal of Consumer Affairs*, 2007,41(1):100-126
- [39] Hajli N., Lin X. Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information[J]. *Journal of Business Ethics*, 2016,133(1):1-13
- [40] United States Federal Trade Commission. Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress[EB/OL]. <http://www.ftc.gov/os/2000/05/index.htm#22.>, 2000
- [41] Yang S., Wang K. The Influence of Information Sensitivity, Compensation on Privacy Concern and Behavioral Intention[J]. *Advances in Information Systems*, 2009,40(1):38-51
- [42] 朱慧,刘洪伟,陈丽,等. 网络用户的信息隐私边界及其敏感度等级研究[J]. *广东工业大学学报*, 2013,30(4):26-32
- [43] 李睿,张锐剑,李文立,等. 移动互联网环境下的隐私泄露容忍度测度方法[J]. *管理评论*, 2016,28(7):102-111
- [44] 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[J]. *系统工程理论与实践*, 2012,32(10):2186-2197

*How does Work Engagement Transmit from Supervisors to Subordinates:
The Test of a Trickle-Down Model*

Xie Baoguo¹, Guo Yongxing² and Xia De¹

(1.School of Management, Wuhan University of Technology, Wuhan 430070;

2.School of Psychology, South China Normal University, Guangzhou 510631)

Abstract: Under the logic of the trickle-down model, this study examines whether and how work engagement transmits from team leaders to their direct followers. In order to reduce the common method bias, the time-lagged sampling is used to collect data. The participants are customer services employees working in a call centre of a large state-owned telecom company in China. Hierarchical Linear Mode (HLM) is used to test the hypotheses. The results show that: (1) team leaders' work engagement is positively related to their followers' work engagement, (2) followers' work meaningfulness mediates the relationship between leader's work engagement and followers' work engagement, (3) empowering leadership moderates the relationship between work meaningfulness and subordinates' work engagement, and (4) the indirect effect of work meaningfulness is moderated by empowering leadership. In the end, some theoretical and managerial implications are offered, and limitations and future directions are discussed.

Key words: trickle-down model, work engagement, work meaningfulness, empowering leadership

(上接第 107 页)

*The Influence Mechanism of Privacy Policies on Consumers' Willingness to Provide Information:
Based on Moderating Effects of Information Sensitivity*

Liang Xiaodan, Li Yinghao and Liu Fang

(School of Business Administration, Zhejiang Gongshang University, Hangzhou 310018)

Abstract: Based on the signaling theory and CPM theory, this paper examines how the contents of online privacy policies influence the consumers' willingness to provide personal information and the moderating effects of information sensitivity through three between-subjects experimental designs. The results demonstrate that the notification clarity, permissiveness and protection degrees offered by privacy policies have significant impacts on consumers' perceived information control and perceived privacy risk. Information sensitivity moderates the correlations between permissiveness, protection degrees offered by a privacy policy and consumers' perceptions. The results also reveal that perceived information control has a significant positive influence on the willingness to provide personal information, and the willingness is also influenced by perceived privacy risk negatively.

Key words: online privacy policy, perceived information control, perceived privacy risk, information sensitivity