

网络社交平台用户隐私披露与多主体协同保护研究

丁舒姮

扬州大学商学院, 江苏 扬州

收稿日期: 2025年2月5日; 录用日期: 2025年2月17日; 发布日期: 2025年3月7日

摘要

随着互联网社交普及, 用户隐私披露类型多样, 但同时面临着自我披露、应用服务商不当操作、黑客攻击等风险。通过线上线下问卷调查303份, 发现用户隐私保护意识不均衡, 对平台安全认知保守且泄露风险高等问题。原因在于隐私保护立法滞后、多部门协同机制缺失、平台自治规范成效差。为此提出完善协同治理机制、细化法律法规、加强企业管理与技术水平、增强公民意识等对策, 旨在构建良好网络隐私保护生态。

关键词

社交平台, 隐私披露, 协同保护, 多元主体

A Study on Online Social Platform Users' Privacy Disclosure and Multi-Stakeholder Collaborative Protection

Shuheng Ding

Business School of Yangzhou University, Yangzhou Jiangsu

Received: Feb. 5th, 2025; accepted: Feb. 17th, 2025; published: Mar. 7th, 2025

Abstract

With the widespread use of internet-based social interactions, the types of user privacy disclosures have become more diverse. However, users are simultaneously facing risks such as self-disclosure, improper handling by app service providers, and cyber-attacks. Based on 303 online and offline questionnaires, the study reveals uneven user awareness of privacy protection, conservative perceptions

of platform security, and high risks of data leakage. Contributing factors include lagging privacy protection legislation, the absence of multi-departmental coordination mechanisms, and ineffective self-regulation by platforms. Proposed countermeasures involve improving collaborative governance mechanisms, refining legal frameworks, enhancing corporate management and technological capabilities, and strengthening public awareness, aiming to establish a robust ecosystem for online privacy protection.

Keywords

Social Platforms, Privacy Disclosure, Collaborative Protection, Multi-Stakeholders

Copyright © 2025 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

随着互联网社交网络的日益普及，人与人之间的交流逐渐从实际的物理空间转移到互联网的虚拟网络世界。中国互联网络信息中心(CNNIC)在第 54 次《中国互联网络发展状况统计报告》指出，截至 2024 年 6 月，我国网民规模达 11 亿人，相比于 2023 年 12 月，增长了 742 万人。在进行网络社交时，一方面，人们感知到隐私风险而积极保护个人隐私，他们主要通过选择信任的媒体平台、谨慎注册填写、设置复杂且差异化密码等方式管理和保护个人隐私；另一方面，社交媒体鼓励人们披露自我、交换信息。人们基于各种各样的原因，进行着大量的自我披露。然而面对强大的网络数据，个人隐私保护能力微不足道，还需要多主体协同参与共同营造良好的网络环境。

2. 网络社交平台用户隐私披露的类型、存在的风险

2.1. 网络社交平台用户隐私披露的类型

2.1.1. 个人基本信息披露

身份信息。包括姓名、性别、年龄等。在一些社交平台的个人资料设置中，用户可能会填写自己的真实姓名。有些平台甚至会要求实名认证。用户在社交互动过程中也会在聊天、评论等场景下无意或有意地透露自己的性别和年龄等信息。

联系方式。主要是电话号码和电子邮箱。部分社交平台在注册过程中会要求用户绑定手机号，用于账号安全验证等目的。

地理位置信息。带有定位功能的社交平台在用户使用基于位置的服务时会披露地理位置。需要注意在一些旅游社交平台上，用户会发布自己在某个著名景点的打卡动态，同时附上位置信息。

2.1.2. 社交关系信息披露

社交平台中的好友列表详细记录了用户的社交连接，属于敏感隐私信息。部分平台可能因默认设置或在用户授权第三方应用时将好友列表信息共享出去。

2.1.3. 行为和偏好信息披露

社交平台会精确记录用户的浏览轨迹，包括所查看的个人主页、文章、视频等内容。这些浏览记录能够清晰反映用户的兴趣爱好和关注焦点。点赞和评论行为则直观展现了用户对特定内容的态度和偏好。

2.2. 网络社交平台用户隐私披露存在的风险

通过对相关文献的梳理和分析, 社交平台作为虚拟互动空间, 其用户身份隐匿性和信息分散化的特征使得隐私披露呈现出较强的不确定性。部分用户高估了自身的风险防控能力, 认为能够有效规避隐私泄露带来的不良影响而忽略隐私风险。

2.2.1. 用户过度自我表露导致的隐私失控

张宁等人研究发现, 为了维系社交网络存在感及寻求他人认同, 用户倾向于主动披露个人位置信息、生活状态及情感体验等私密内容[1]。这种隐私信息的自主暴露为不法分子提供了可乘之机。尤其在基于位置服务的社交场景中, 一旦发生信息泄露, 极易引发人身安全威胁或商业骚扰等严重后果。

2.2.2. 应用服务商存在对已披露信息的不当使用

齐晓娜等人通过分析平台隐私条款发现, 部分平台利用用户主动或被动披露的个人数据进行商业变现, 包括定向广告投放及数据交易等违规行为[2]。这些企业通常以提供服务为由, 在用户使用过程中设置不合理的授权条款, 变相强制获取通讯录等广泛权限, 致使用户隐私遭受侵害, 损害了用户的合法权益。

2.2.3. 黑客针对已披露信息实施攻击

社交平台汇集了大量具有经济价值的用户隐私数据, 已成为黑客重点攻击目标。不法分子可能利用平台技术漏洞或用户在公共网络环境下的信息披露行为, 通过恶意程序窃取敏感数据。王树义的研究表明特别是在社交媒体影响力不断提升的背景下, 黑客开始利用技术手段制造虚假用户评价, 将知名平台作为僵尸粉丝攻击的重点目标, 对用户隐私安全与平台生态造成严重威胁[3]。

3. 网络社交平台用户隐私保护存在的问题

本文采用问卷调查的方式, 对当前移动社交网络用户的行为习惯、隐私关注现状等展开研究, 以揭示网络社交平台用户隐私保护存在的问题。

3.1. 调查工具及问卷设计

本研究通过线上及线下渠道开展问卷调研, 以探究社交平台用户的隐私意识及行为特征。调查问卷设计涵盖定量与定性题项, 包含选择题及开放性问题等多种形式。问卷结构分为三个维度: 基本信息, 调查受访者的基础属性与对数据隐私的认知水平; 隐私感知与态度评估, 考察用户对移动社交媒体可信度、安全性的主观评价以及其对个人信息保护重要性的认识程度和隐私风险归因; 隐私保护实践行为, 分析用户在平台使用过程中的防护措施选择。

本次调查共回收有效样本 303 份, 其中男性和女性受访者占比分别为 56.44%和 43.56%, 样本年龄跨度覆盖青少年至中年群体, 体现出较好的统计学代表性。该问卷旨在从用户认知与行为的双重维度, 系统考察网络社交平台用户隐私保护存在的问题。

3.2. 结果分析

根据问卷调查结果与数据分析, 当前网络社交平台用户隐私保护存在以下突出问题。

3.2.1. 用户隐私保护意识不均衡

调查显示, 用户对位置信息(79.87%)、浏览记录(67%)等行为关联数据的保护意识显著高于设备信息(60.07%)和身份信息(57.43%)。这种关注度的差异表明用户对不同类型的隐私信息采取的保护措施存在明显割裂, 部分敏感数据(如身份信息)的防护意识薄弱。

3.2.2. 用户主动防护行为不足

66.34%的受访者指出“用户对个人数据保护的重视程度不足”是隐私泄露的重要原因。尽管部分用户采取设置复杂密码、谨慎注册等基础防护措施,但面对平台诱导性设计(如默认开启定位功能)或社交需求驱动下的过度自我表露,用户主动规避风险的意愿与能力仍显不足。

3.2.3. 用户对平台安全性的信任度不足

仅有 46.2%的受访者认为社交平台“非常安全”或“比较安全”,而超过半数用户(53.63%)对平台安全性持消极态度。此外,43.56%的用户确认遭遇过隐私泄露,39.27%的用户表示“不确定”,反映出用户对平台安全防护能力的普遍质疑,进一步削弱了用户信任。

3.2.4. 商业机构过度收集与滥用用户数据

72.94%的受访者认为“商业机构过度收集利用数据”是隐私保护的主要问题。部分平台通过模糊的隐私条款强制获取用户权限,利用数据进行定向广告投放或交易,甚至存在未经授权共享用户社交关系链(如好友列表)等行为,严重侵害用户合法权益。

3.2.5. 隐私泄露风险与维权难度高

调查中 82.84%的用户面临实际或潜在的隐私威胁。用户普遍反映维权渠道不畅、法律救济成本高,导致隐私泄露事件发生后难以有效追责,进一步加剧了用户对隐私保护体系的失望情绪。

4. 网络社交平台用户隐私保护存在问题的原因分析

4.1. 隐私保护立法保障不足

随着网络社交平台的发展,个人信息在采集、存储、传输等环节存在被非法获取与监控的风险。当前我国隐私权保护立法体系存在滞后性。近六成受访者认为“现有隐私保护相关法律体系尚未健全”。这一现象的根源在于我国隐私权保护立法相对滞后,实践经验与理论研究的积累不足,导致法律规范的制定与完善进程缓慢。尽管已实施《个人信息保护法》已实施,但网络社交平台领域存在用户数据呈现出体量大、类型繁多、流动频繁等特点,传统隐私保护规则难以为用户提供充分保护。此外,跨平台数据共享、算法推荐、用户画像等新兴业态的出现,加剧了隐私保护的复杂性,而相应的法律规制未能及时跟进,形成了保护真空。根据 2023 年最高人民法院工作报告,侵犯公民个人信息案件的维权成功率仅为 35.6%,反映出法律执行层面仍存在诸多障碍。

4.2. 隐私保护多部门协同机制尚未健全

在大数据背景下,由政府作为核心主体的隐私保护领域由于市场信息的繁杂,处置能力正受到制约。高达 43.56%的受访者确认遭遇过个人隐私泄露,39.27%的受访者表示“不确定”是否遭遇过泄露,如此高的潜在泄露比例反映出当前监管体系的不足。现行体制下,尽管工信部、电信管理部门、公安机关和司法部门等均在其职责范围内制定了相关管理规范,但这种分散的监管架构导致隐私侵害事件发生时,由于相关信息分散在多个部门而职责推诿的情况。部门间职责认定和目标定位方面存在不明确现象,部门间协作机制匮乏[4]。问卷表明有近半数的用户迫切希望“建立跨平台数据共享的安全标准”。同时,现有的多部门治理模式存在重复监管与监管缺位的双重问题,部分领域出现重复执法,造成行政资源浪费;而监管主体的多元化反而导致某些隐私信息处于监管盲区,增加了隐私泄露风险。

4.3. 平台自治规范机制成效不彰

在众多国内社交平台中,虽然普遍制定了隐私保护相关条款,但多为单方面的约定,内容笼统且缺

乏与用户的平等协商。具体表现在：一是规范制定层面，平台倾向于制定模糊的隐私条款，为数据使用预留较大操作空间。中国消费者协会的调查显示，主流社交平台的隐私政策平均阅读难度相当于大学水平，普通用户难以理解；二是执行监督层面，70.3%的用户呼吁“规范企业对用户数据的采集和使用行为”。由于缺乏第三方评估机制，平台自查自纠流于形式；三是行业协同层面，平台间数据使用标准不统一，缺乏行业自律组织统筹。由于网络社交领域未能构建有效的规范体系，一些主要平台无法肩负起引领带头的责任，各平台之间缺少统一的操作规范和行为准则[5]。这种规范缺位直接导致了平台信用不足的问题。在缺乏有效约束的情况下，用户数据权益保护难以得到有效保障。

4.4. 公民隐私保护意识薄弱

网络当前公民隐私保护意识薄弱的现象，根植于多重社会与技术因素。首先，隐私教育体系不健全是核心原因之一。我国基础教育与公共宣传中缺乏系统化的隐私保护课程，导致公众对隐私泄露的潜在危害认知不足。调查显示，仅 38.4%的受访者能准确识别常见的隐私陷阱，反映出公众缺乏应对风险的必要知识储备。其次，平台界面设计存在诱导性，加剧了用户疏忽。社交平台常通过简化隐私设置流程、默认开启数据共享功能或采用“同意疲劳”策略，促使用户在追求便捷性时降低警惕。此外，文化因素与社交需求驱动也削弱了隐私保护意识。部分用户为获取社交认同或参与特定活动(如位置打卡、兴趣社群)，主动披露敏感信息，甚至将隐私让渡视为社交“入场券”。

5. 网络社交平台用户隐私协同保护的对策建议

5.1. 完善公民隐私保护协同治理机制

在当代网络空间治理体系的构建过程中，隐私保护的协同机制需要关注政府内部各职能部门之间的协作关系，并强化与非政府机构之间的深度伙伴关系。就政府治理层面而言，建议建立由网信办牵头，公安、工信、市场监管部门参与的联席会议制度，制定《社交平台数据共享安全标准》。通过科学界定各部门的职责边界，进而构建起反应迅速、运转高效的联动、信息共享机制。技术支撑层面而言，组建跨部门技术专家团队，每季度对新型隐私威胁进行评估，并建立统一的隐私事件处置系统。各职能部门应当联合攻关大力推进隐私防护技术创新，完善数据安全平台的建设。引入专业机构定期对平台隐私保护措施进行评估，设立隐私保护评级体系，对评级较差的平台进行重点监管。此外，政府部门在推进治理工作的过程中还应当高度重视对网络安全人才的吸纳与培养[6]，借助多元化力量的积极参与来共同营造良性的网络生态环境。

5.2. 细化隐私保护的法律法规

本次调查中占 63.37%的受访者认为应该加强法律对社交平台中个人信息的保护，在我国现行隐私保护法律体系的发展进程中，取证难度高、监管效能不足以及行业发展动态等多重因素制约着法治建设的推进步伐。从法律规范角度而言，制定《社交平台用户数据采集规范》，明确基础信息和敏感信息的采集标准，规定数据存储期限。明确平台违规使用用户数据的具体处罚标准，对泄露隐私的行为按泄露数据量分级处罚，并设立惩罚性赔偿制度。同时，建立个人信息侵权案件快速审理通道。就责任主体而言，法律法规需要准确界定政府部门、企业平台、个体用户在信息保护过程中的权责边界。同时，应当建立专门的信息安全监管机构，构建科学完备的技术防护体系。通过多维度的法律规制，最终实现对公民个人隐私的全方位保护。

5.3. 加强企业自我管理机制和技术水平

第一，企业作为海量用户个人信息的主要持有者与管理者，必须在现有法律法规的严格约束下，构

建专业化的信息安全管理部门,通过系统性的制度设计来防范各类信息安全风险[7]。第二,企业平台应建立分级防护体系,将用户数据分为一般(基础信息)、重要(位置数据)、核心(生物特征)三级,针对不同级别采用不同加密强度和访问权限控制。同时部署 AI 异常行为检测系统,提升安全防护能力。严格把控个人信息收集与使用的合理边界,并积极参与行业标准的制定与完善工作。第三,建立多元化的用户投诉反馈渠道。搭建便捷高效的投诉平台、引入专业的第三方监督力量。承诺 24 小时内响应隐私相关投诉,并定期发布用户满意度报告,以便企业能够更加及时地发现并有效解决各类信息安全隐患[8],最终构建起全方位、多层次的用户隐私保护网络体系,为网络空间治理提供有力支撑。

5.4. 增强公民个人隐私保护意识

移动社交网络用户普遍认为提升个体隐私防范意识(占 62.71%)已成为规避信息泄露风险的关键环节。在此背景下,用户须深入把握信息分享的潜在影响,审慎处理敏感数据。针对不同年龄段用户,应设计差异化的隐私保护课程,通过短视频平台推送隐私保护小贴士,并在社区开展定期讲座。同时,开发隐私健康评估工具,帮助用户定期检查隐私设置,提供一键隐私配置功能,实现快速设置推荐方案。在面对信息侵权事件,用户理应积极维权。政府和企业应积极倾听公众意见,开展隐私保护宣传和教育,让公众了解到隐私保护的重要性[9]。同时,公众对隐私问题的监督也能促进政府和企业提高隐私保护水平。

基金项目

扬州大学科创基金项目:“网络社交平台用户隐私披露与多主体协同保护研究”(项目编号:XCX20240946)研究成果。

参考文献

- [1] 张宁,赵来娟,何渊.大数据环境下移动社交网络用户隐私问题研究[J].情报探索,2019(1):14-17.
- [2] 齐晓娜,张宇敬,封二英.移动社交网络用户隐私保护问题研究[J].产业与科技论坛,2017,16(16):35-36.
- [3] 王树义,朱娜.移动社交媒体用户隐私保护对策研究[J].情报理论与实践,2013,36(7):36-40.
- [4] 李哲雅.大数据时代公民隐私权利保护问题研究[D]:[硕士学位论文].北京:华北电力大学,2021.
- [5] 王跃娇.个人信息安全乱象的协同治理机制研究[D]:[硕士学位论文].上海:上海师范大学,2017.
- [6] 狄振鹏,姜士伟.大数据时代政府数据开放与公民隐私保护问题研究[J].情报杂志,2022,41(2):155-159+118.
- [7] 应雨轩.大数据时代我国公民个人信息保护的协同研究[D]:[硕士学位论文].上海:华东政法大学,2023.
- [8] 尹异凡.社交平台用户隐私信息披露影响因素研究[D]:[硕士学位论文].吉林:吉林大学,2021.
- [9] 邵云娜,项邦孟.构建数据安全协同治理制度体系的路径与策略[J].电脑知识与技术,2023,19(26):66-69.