Proceedings of the 2nd International Conference on Interdisciplinary Humanities and Communication Studies
DOI: 10.54254/2753-7064/24/20231616

Research on the Disclosure of Personal Privacy by Social Media Users in the Era of Big Data and Mobile Internet, and Countermeasures

Haochen Liu[1,a,*]

[1]*MONASH University, Unit/5 1522 Malvern Rd, Glen Iris VIC 3146, Australia*
a. 1282803276@qq.com
**corresponding author*

Abstract: In the epoch of big data and the ubiquity of mobile internet, the sanctity of personal privacy on social media platforms is increasingly imperiled. As communicative exchanges on these platforms become nearly instantaneous and pervasively ubiquitous, the demarcation between corporeal experiences and digital interactions becomes increasingly nebulous, thereby augmenting the intricacy of privacy conundrums. The digital transmutation and incessant circulation of personal datum, magnified by avant-garde big data technologies, intensify the vulnerabilities surrounding user confidentiality. Concurrently, societal conceptualizations of privacy undergo a paradigmatic shift, compelling a recalibration between the imperatives of privacy preservation and the exigencies of personal information exploitation. This investigation offers a perspicacious dissection of the historical trajectory of privacy, elucidates the manifold challenges engendered by the disclosure propensities of social media aficionados, and delineates prospective regulatory paradigms. The overarching aspiration is to promulgate efficacious stratagems for safeguarding personal privacy on social media amidst the contemporary digital renaissance.

Keywords: Mobile Internet, Big Data, Social Media, Personal Information, Privacy

1. Introduction

Since the 20th century, the rapid evolution of internet technology has ushered in the era of big data and mobile internet. These technologies have deeply influenced the processes of data collection, storage, and utilization across numerous sectors [1]. In contemporary society, the amalgamation of powerful smart devices, a plethora of service applications, and swift expansion of network connectivity has substantially heightened the risk of online users' privacy breaches, whether intentional or inadvertent [2].

Current academic discourse displays an escalating interest in the study of personal privacy disclosure and corresponding countermeasures within the realm of mobile internet. This domain has burgeoned over time, further enriching our understanding and insights [3]. The 1960s marked a pivotal moment with the global surge of the internet, catalyzing the evolution of mobile internet communications. The subsequent introduction of wireless access by carriers coupled with rapid advancements in mobile internet technology has resulted in monumental leaps in modern mobile communications [4]. In the prevailing era of social media, individuals predominantly resort to devices

© 2023 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7064/24/20231616

such as smartphones and tablets to access the mobile internet. This facilitates the swift dissemination of a voluminous amount of information, intertwining various facets of daily life [5]. A report by the China Internet Network Information Center (CNNIC) unveiled on March 2, 2023, indicates that as of December 2022, the number of online users in China escalated to 1.067 billion, marking an augmentation of 35.49 million from December 2021. This corresponds to an internet penetration rate of 76.6% [6]. Such metrics accentuate the significant surge in internet user base. The ubiquitous adoption of the internet combined with the evolution of modern media information technology has thrust the digital era into an epoch of pronounced expansion [7].

Eminent scholars, such as Daniel Solove, have postulated this era as the "privacy-unprotected era," introducing concepts such as "zero privacy" [8]. In the mobile internet age, the definition of personal privacy pivots around the proprietary nature of personal information and data, which is discernibly distinct from conventional notions of privacy. This encapsulates personal details ranging from names, phone numbers, and home addresses to occupations, ID numbers, and confidential passwords [9]. However, the metamorphosis of the internet has engendered significant shifts in the dimensions, attributes, manifestations, and protection modalities of privacy. Instances encompass internet-based doxxing, which has stoked societal apprehensions, the proliferation of private message leaks through screenshot-sharing, misuse of facial recognition technology in public domains like hotels, banks, and airports, and the propensity of social media applications to gather user data and autonomously dispatch associated content. These evolving privacy concerns underscore the palpable breaches of individual privacy in the digital domain [10]. This necessitates a holistic reassessment of the formidable challenges poised against personal privacy in the contemporary societal and technological milieu and the foundational metamorphoses unfolding in the internet age.

The primary objective of this research is a methodical scrutiny and dissection of the pertinent academic contributions in this arena. By anchoring on the cornerstones of big data, mobile internet, social media, privacy security, privacy disclosure challenges, and the prevailing societal framework, this study probes into the contemporary manifestations of personal privacy disclosure and its potential counteractive measures. The ambition is to furnish readers with a lucid understanding of the dynamic evolutions and pivotal trajectories in this domain.

2. Literature Review

2.1. Privacy

In contemporary America, the concept of privacy is multidimensional, and scholars have presented diverse interpretations and definitions. A pivotal idea that emerges is that of "control" [11]. In particular, some American academics argue that privacy symbolizes "control over personal information" [12]. This notion of privacy is highly adaptive, evolving alongside shifts in information communication technology. As a result, the very essence of privacy corresponds with the technological landscape of its time. This dynamic has led to an expansion in the conceptual boundaries of privacy as information communication technology has advanced. Originally perceived as a right to solitude, the concept of privacy has now metamorphosed into a countermeasure to the challenges that economic and technological developments pose to human rights [13].

Vincent [14] provides a detailed chronology of privacy in his work, "A History of Privacy." He demarcates its evolution into five distinct epochs: the pre-privacy era (1300-1650), the era of privacy coupled with communication (1650-1800), the period of prosperity (1800-1900), modernity (1900-1970), and the digital age (1970-2015). Moreover, he remarks, "The decline of privacy was initiated in the mid-1960s, characterized by burgeoning debates and literature on the subject" [15].

Technological strides have shifted privacy's locus from tangible spaces to the digital domain [16]. During the 1920s and 1930s, the ascendance of printing technology and the telegraph transformed

DOI: 10.54254/2753-7064/24/20231616

newspapers into principal information sources. Concurrently, the surge in tabloid newspapers and advances in photography posed novel challenges to individual privacy [17]. By the 1960s, the advent of computer technology meant digital data began to supersede textual records as the predominant medium for information documentation and storage. This evolution accelerated the pace of information gathering, rendering data storage and retrieval more versatile, and, in the process, reshaping the contours of personal privacy [18]. Vincent emphasized in the 1970s that the meaning of privacy transitioned to spotlight individual anonymity over the sanctity of private spaces.

With the dawn of the social media age, the ubiquity of social networks and the mobile internet created a novel paradigm. Individuals commenced generating content and disseminating personal data, while potent entities like governments and corporations intensified their data collection efforts, thereby challenging age-old privacy paradigms [19]. Nissenbaum [20] introduced the concept of contextual integrity concerning privacy. She stressed that emerging technologies' impact on privacy should be contextualized, advocating for a harmonious integration of privacy principles within tangible contexts.

The 21st century heralded the smart media age, where the emergence of digital identities rendered personal data a pivotal component of privacy [21]. Data harvesting methods have become more covert and exhaustive. Contemporary social media platforms perpetually monitor users' activities, both online and offline. The potency of data analytics has surged, allowing for the precise unearthing of obscured personal information via big data's correlation and predictive capabilities [22]. Chinese academic, Wang Junxiu, underscores that the "informationalization of privacy" and the "privacyization of information" epitomize the hallmarks of the digital era [23]. Some academics contend that privacy has transitioned from a static construct to a fluid entity, necessitating a context-sensitive evaluation [24]. It's posited that comprehensive privacy is progressively supplanting biological privacy. At the same time, concerns are raised that big data analytics might inadvertently expose personal details [25]. Some scholars note the increasing subtlety and scale of privacy breaches [26]. With relentless advancements in groundbreaking technologies like big data and artificial intelligence, the smart era brings forth fresh challenges to privacy norms, redressal mechanisms, and tenets of autonomy. Privacy's essence is also in flux, transitioning from an individual-centric data control model to one emphasizing societal control [27].

2.2. Privacy Disclosure Behavior of Social Media Users

Personal disclosure pertains to the act of users revealing personal information, be it intentional or unintentional. This information can range from personality traits and interests to life experiences and future plans [28].

The behavior of privacy disclosure among social media users is shaped by numerous determinants. Current scholarly works predominantly zone in on three main aspects of this behavior:

Motivational Aspects: Studies have delved deep into the underlying motivations that push social media users towards privacy disclosures [29]. The indispensable role of social media in the lives of its users is evident, as it offers instant gratification, emotional succor, and valuable social capital [30]. The motivations driving social media utilization align closely with users' emotional needs [31]. Further, social media platforms facilitate users in carving out their online personas and partake in resource exchanges [32]. In the process of utilizing these platforms, users, driven by their motivations, are often inclined to disclose facets of their personal lives. Such motivations encompass the aspiration to swiftly narrow down interpersonal gaps, sustain bonds, amass social capital, and augment opportunities. Academics have identified the construction of social networks, the quest for economic gains, the inclination towards self-realization, and the drive to augment discursive authority as the primary drivers behind such disclosures [33].

DOI: 10.54254/2753-7064/24/20231616

Determinants of Disclosure Behavior: Another realm of exploration is the set of factors that impact the privacy disclosure behaviors of users [34]. Findings suggest that individuals who encounter heightened instances of privacy infringements may exhibit amplified privacy apprehensions, especially if they possess a robust demand for informational privacy [35]. Yet, an escalation in the demand for information privacy doesn't invariably translate into alterations in ensuing disclosure behaviors [36]. The degree of trust harbored by users encapsulates their psychological trade-offs between perceived risks and rewards, inclusive of the perceived benefits derived from personalized information. The concerns surrounding privacy are intertwined with users' valuation of personalized information. Recognizing the worth in personalized content galvanizes trust establishment. Other pivotal determinants include emotional responses and gender [37]. Building on this, some scholars postulate a negative interrelation between privacy apprehensions and the volume, depth, and genuineness of social media disclosures. However, individual stress levels can temper this linkage, with elevated stress levels diminishing the adverse influence of privacy concerns on the extent and depth of disclosures [38]. Furthermore, the stress-induced moderating effect showcases variation across genders. Pertinent studies underscore that in the virtual social milieu, a fatalistic emotional bond to personal privacy oversight correlates positively with interpersonal privacy stewardship [39].

Perception of Privacy Risks: The final focus area of research orbits around the determinants that shape users' cognizance of privacy-related threats [40]. A subset of studies accentuates the lag in users' risk perception, highlighting the need for amplified cognitive awareness of holistic privacy. Certain users might exhibit a lack of alertness towards privacy challenges, display inconsistent psychological stances, and may not possess an adequate grasp of the modus operandi of data utilization by platforms and the potential ramifications of privacy breaches [41]. Another line of thought, emerging from the vast world of big data, suggests that users may juxtapose privacy breaches as a newfound risk, ranking them lower on the threat spectrum in comparison to more tangible threats like criminal activities or health hazards [42].

2.3. Challenges and Reasons for Social Media Platform Privacy Issues

The task of ensuring privacy for social media users presents a myriad of challenges. One prominent concern arises from generational differences in values and behaviors regarding online privacy [43]. For instance, scholars argue that older generations tend to gravitate towards collectivist cultural values, while younger generations lean more towards individualistic values [44]. This divergence in values can lead to misunderstandings and confusions among younger users about managing their online privacy.

Attempting to dissect the underlying reasons for such challenges, the academic community has introduced the concept of "privacy cynicism." This refers to the prevailing sentiment among users where they harbor negative perceptions about how online platforms manage and protect user data. Such cynicism often manifests in feelings of distrust, uncertainty, powerlessness, and a begrudging compliance with the status quo, further complicating efforts to bolster privacy protections on these platforms [45].

From a broader perspective, some scholars posit that the omnipresence of social media platforms has effectively digitized Bentham's concept of the "panopticon" – an all-seeing surveillance system – where breaches of user privacy are not only rampant but have also become alarmingly normalized [46]. Adding another dimension to this issue, some argue that the free services proffered by tech companies invariably come at the expense of user privacy. Given the colossal technological and financial clout these entities wield, individual users, especially vulnerable demographics such as teenagers and those with limited media literacy, often find themselves in compromised positions, with little recourse to assert their privacy rights [47].

DOI: 10.54254/2753-7064/24/20231616

2.4. Regulatory Pathways for Personal Privacy Leakage on Social Media Platforms

The academic community generally classifies the entities that govern social media into three primary categories: governments, corporations, and civil society [48].

From the perspective of government oversight, some posit that the imminent issues pertaining to social media governance will largely hinge on regional autonomy spearheaded by national governments [49]. Conversely, within the sphere of corporate governance, it's believed that internet corporations set and control the entire framework governing user behavior on social media platforms. This grants these corporations immense influence over various pivotal junctures [50]. Some analysts further suggest that these platforms have a unilateral power to enforce order [51]. As for governance by civil society, multi-stakeholder involvement is deemed necessary to formulate universally accepted and actionable solutions. Here, international forums and non-governmental organizations play instrumental roles [52].

The focal points of academic inquiries into social media governance encompass misinformation, infringement of personal privacy, violation of intellectual property rights, and platform monopolization [53]. In terms of misinformation, emphasis is placed on issues like fake news, falsehoods, rumors, extremist content, and explicit material found on social media platforms [54]. Fake news, especially, has attracted considerable attention due to its rapid dissemination, often outpacing verified information. This phenomenon demands a synergistic approach, utilizing both technological and societal interventions [55]. On the subject of extremist content, the discourse underscores the imperative for immediate governance, given the profound challenges confronting global oversight. There's also been noteworthy progress in safeguarding minors from explicit content on these platforms [56].

When addressing personal privacy breaches, research primarily zeroes in on the methodologies adopted by attackers, strategies for privacy protection, and the dimensions of user privacy safeguards [57]. A common modus operandi among malicious actors involves collating fragmented personal data to reconstruct comprehensive user profiles, which could lead to dire implications. Concerning privacy protection, significant emphasis has been placed on safeguarding user location data. Meanwhile, a number of studies have delved into the extent to which users utilize privacy settings, revealing that a significant portion neglects to fully exploit the privacy tools available on these platforms [58].

Intellectual property rights on social media platforms, particularly copyrights, are of paramount importance. While content creators hold the copyrights for original content, platforms retain specific rights over their usage. Despite some countries updating their legislation to align with the evolving dynamics of social media, there remains a discernible gap between legal frameworks and technological progression. This underscores the need for enhanced international legal instruments and enforcement mechanisms to safeguard intellectual property online [59].

With respect to the monopolization of platforms, scholars argue that phenomena such as network effects, lock-in effects, and platform effects have culminated in a monopolistic internet landscape. While such monopolies might initially usher in innovations, in the long run, they might stifle competition and yield unfavorable outcomes [60].

In summary, the regulatory pathways for social media governance encompass legal measures, technological means, and company regulations. Legal measures include international laws and regulations as well as domestic regulatory measures in various countries. At the international level, an international legal framework adapted to social media governance has yet to be established, and governments worldwide face challenges in addressing the legal and enforcement issues related to social media governance. Technological means of governance involve using technology and algorithms to regulate and influence content and behaviors on social media. Some scholars are concerned about the potential bias in algorithmic filtering mechanisms, as algorithms may lead to

DOI: 10.54254/2753-7064/24/20231616

information manipulation and platform bias. Finally, company regulations emphasize the importance of self-management and oversight by social media companies themselves, as these companies play a crucial role in the day-to-day governance and handling of their platforms.

In conclusion, social media governance is a multi-faceted process involving a wide range of issues, diverse governing entities, and various governance methods. While there is already a substantial body of research covering these aspects, the entire process still requires more systematic attention.

3. Conclusion

This paper has undertaken a comprehensive exploration of the issue of privacy, encompassing its historical evolution, influencing factors, and the regulatory pathways pertaining to the disclosure of personal privacy by social media users and the leakage of individual privacy on social media platforms in the era of big data and mobile internet. The origins of privacy issues and the challenges surrounding their protection are closely intertwined with technological and societal developments. This constitutes a continually evolving and intricate domain, shaped by the interplay of technological, societal, and individual factors. Concurrently, social media plays a pivotal role in the lives of users, serving as a means to attain immediate gratification, emotional support, and social capital. However, users often exhibit a comparatively low perception of the risks associated with privacy protection. With the advent of the era of intelligent media, there is an imperative need to reevaluate the conceptualization and protective mechanisms of privacy to effectively adapt to the ever-changing landscape of social media. In the context of privacy infringements in the era of big data, there is a notable disparity in the perceived risk by users, highlighting the necessity for extensive education and awareness campaigns aimed at augmenting users' privacy protection consciousness. Simultaneously, from a regulatory perspective, governments, corporations, and civil society all constitute principal agents in the governance of social media. Consequently, safeguarding privacy necessitates not only policy and technological support but also an elevation of privacy awareness and capabilities among corporate users and individuals, with the aim of achieving social control and individual autonomy over privacy.

References

[1] *van Ooijen, I. et al. (2022). Privacy cynicism and its role in privacy decision-making. Communication Research. https://doi.org/10.1177/00936502211060984*

[2] *Acquisti, A. et al. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509-514. https://doi.org/10.1126/science.aaa1465*

[3] *Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. First Monday, 11(9). https://doi.org/10.5210/fm.v11i9.1394*

[4] *Joshi, R. et al. (2022). Internet an integral part of human life in 21st century: A review. Current Journal of Applied Science and Technology, 2022 - Volume 41 [Issue 36], 12-18. https://doi.org/10.9734/cjast/2022/v41i363963*

[5] *Auer, M. R. (2011). The policy sciences of social media. Policy Studies Journal, 39(4), 709-736. https://doi.org/10.1111/j.1541-0072.2011.00428.x*

[6] *China Internet Network Information Center (CNNIC). (2023). The 51st statistical report on China's internet development. www.cnnic.com.cn/IDR/ReportDownloads/202307/P020230829505026163347.pdf*

[7] *Mantelero, A. (2016). From group privacy to collective privacy: Towards a new dimension of privacy and data protection in the big data era. In Group Privacy (pp. 139-158). https://doi.org/10.1007/978-3-319-46608-8_8*

[8] *Solove, D. J. (2008). The future of reputation: Gossip, rumor, and privacy on the internet. Yale University Press.*

[9] *Lee, C., & Ahmed, G. (2021). Improving IoT privacy, data protection and security concerns. International Journal of Technology, Innovation and Management (IJTIM), 1(1), 18-33. https://doi.org/10.54489/ijtim.v1i1.12*

[10] *Varshney, S. et al. (2020). Big data privacy breach prevention strategies. 2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (ISSSC). https://doi.org/10.1109/isssc50941.2020.9358878*

[11] Albakjaji, M. et al. (2020). The legal dilemma in governing the privacy right of e-commerce users. International Journal of Service Science, Management, Engineering, and Technology, 11(4), 166-187. https://doi.org/10.4018/ijssmet.2020100110
[12] Albakjaji, M. et al. (2020). The legal dilemma in governing the privacy right of e-commerce users. International Journal of Service Science, Management, Engineering, and Technology, 11(4), 166-187. https://doi.org/10.4018/ijssmet.2020100110
[13] DeCew, J. W. (2018). In pursuit of privacy: Law, ethics, and the rise of technology. Cornell University Press.
[14] Vincent, D. (2016). Privacy: A short history. John Wiley & Sons.
[15] Vincent, D. (2016). Privacy: A short history. John Wiley & Sons.
[16] Di Pietro, R., & Cresci, S. (2021). Metaverse: Security and privacy issues. 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA). https://doi.org/10.1109/tpsisa52974.2021.00032
[17] Lloyd, I. (2020). Information technology law. Oxford University Press.
[18] Lloyd, I. (2020). Information technology law. Oxford University Press.
[19] Mansoor, M. (2021). Citizens' trust in government as a function of good governance and government agency's provision of quality information on social media during COVID-19. Government Information Quarterly, 38(4), 101597. https://doi.org/10.1016/j.giq.2021.101597
[20] Nissenbaum, H. (2009). Privacy in context. Stanford University Press.
[21] Fox, A. K., & Royne, M. B. (2018). PRIVATE INFORMATION in a SOCIAL WORLD: ASSESSING CONSUMERS' FEAR and UNDERSTANDING of SOCIAL MEDIA PRIVACY. Journal of Marketing Theory and Practice, 26(1-2), 72-89. https://doi.org/10.1080/10696679.2017.1389242
[22] Castañeda, J. A. et al. (2007). The dimensionality of customer privacy concern on the internet. Online Information Review, 31(4), 420-439. https://doi.org/10.1108/14684520710780395
[23] Wang, J. X. (2020). Digital society and privacy reshaping: Using "face recognition" as an example. Weixin Official Accounts Platform. Retrieved from mp.weixin.qq.com/s?__biz=MzA4MjcxMDEwNQ==&mid=2686271038&idx=2&sn=e0661313da5849527a66c6943b2830e1&chksm=ba6805088d1f8c1efddd8c9d5359a120c6a545a5a38ae502fe0af4ca71063df6361f99fa3d06&scene=27
[24] Garon, J. (2013). Social media in the workplace from constitutional to intellectual property rights. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2348779
[25] Yi, Z., & Chen, X. (2022). Personal privacy protection problems in the digital age. ArXiv (Cornell University). https://doi.org/10.48550/arxiv.2211.09591
[26] Gadzhiev, H. (2020). Privacy protection in the digital age. Journal of Foreign Legislation and Comparative Law, 5(6), 1-0. https://doi.org/10.12737/jflcl.2019.6.1
[27] P. Romansky, R., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. Mathematical Biosciences and Engineering, 17(5), 5288-5303. https://doi.org/10.3934/mbe.2020286
[28] Siahaan, M. N. et al. (2021). Self-disclosure of social media users in Indonesia: The influence of personal and social media factors. Information Technology & People. https://doi.org/10.1108/itp-06-2020-0389
[29] Li, K., Wang, X., Li, K., & Che, J. (2016). Information privacy disclosure on social network sites: An empirical investigation from social exchange perspective. Nankai Business Review International, 7(3), 282-300.
[30] Li, K. et al. (2015). An empirical analysis of users' privacy disclosure behaviors on social network sites. Information & Management, 52(7), 882-891. https://doi.org/10.1016/j.im.2015.07.006
[31] Xu, H. et al. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. Journal of the Association for Information Systems, 12(12), 798-824. https://doi.org/10.17705/1jais.00281
[32] Xu, H. et al. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. Journal of the Association for Information Systems, 12(12), 798-824. https://doi.org/10.17705/1jais.00281
[33] Haji, I. H. A. et al. (2021). Online private self-disclosure's potential for experiential value co-creation. European Journal of Marketing, 55(12), 3059-3098. https://doi.org/10.1108/ejm-04-2019-0302
[34] Thompson, N. et al. (2021). Do privacy concerns determine online information disclosure? The case of internet addiction. Information & Computer Security. https://doi.org/10.1108/ics-11-2020-0190
[35] Thompson, N. et al. (2021). Do privacy concerns determine online information disclosure? The case of internet addiction. Information & Computer Security. https://doi.org/10.1108/ics-11-2020-0190
[36] Aljohani, M. et al. (2016). A survey of social media users privacy settings & information disclosure. https://doi.org/10.4225/75/58a693deee893
[37] Aribandi, A. et al. (2022). Note: Evaluating trust in the context of conversational information systems for new users of the internet. https://doi.org/10.1145/3530190.3534852

[38] Nazemzadeh, M. (2021). Social media and privacy issues. In Women in Ophthalmology (pp. 319-326). https://doi.org/10.1007/978-3-030-59335-3_40
[39] De Wolf, R. (2019). Contextualizing how teens manage personal and interpersonal privacy on social media. New Media & Society, 22(6). https://doi.org/10.1177/1461444819876570
[40] Alrayes, F. S. et al. (2019). Modelling perceived risks to personal privacy from location disclosure on online social networks. International Journal of Geographical Information Science, 34(1), 150-176. https://doi.org/10.1080/13658816.2019.1654109
[41] Alrayes, F. S. et al. (2019). Modelling perceived risks to personal privacy from location disclosure on online social networks. International Journal of Geographical Information Science, 34(1), 150-176. https://doi.org/10.1080/13658816.2019.1654109
[42] Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. IEEE Security and Privacy Magazine, 3(1), 26-33. https://doi.org/10.1109/msp.2005.22
[43] Bright, L. F. et al. (2022). Social media fatigue and privacy: An exploration of antecedents to consumers' concerns regarding the security of their personal information on social media platforms. Journal of Interactive Advertising, 22(2), 1-16. https://doi.org/10.1080/15252019.2022.2051097
[44] Bright, L. F. et al. (2022). Social media fatigue and privacy: An exploration of antecedents to consumers' concerns regarding the security of their personal information on social media platforms. Journal of Interactive Advertising, 22(2), 1-16. https://doi.org/10.1080/15252019.2022.2051097
[45] van Ooijen, I. et al. (2022). Privacy cynicism and its role in privacy decision-making. Communication Research. https://doi.org/10.1177/00936502211060984
[46] Spiller, K. (2020). 'Putting everything up there': Framing how we navigate the intricacies of privacy and security on social media. Humanity & Society. https://doi.org/10.1177/0160597620904502
[47] Ali, I. et al. (2022). Social media platforms and social enterprise: Bibliometric analysis and systematic review. International Journal of Information Management, 69, 102510. https://doi.org/10.1016/j.ijinfomgt.2022.102510
[48] Chen, S. et al. (2023). Research on the influence mechanism of privacy invasion experiences with privacy protection intentions in social media contexts: Regulatory focus as the moderator. Frontiers in Psychology, 13. https://doi.org/10.3389/fpsyg.2022.1031592
[49] Lappas, G. et al. (2017). Facebook communication strategies and their effectiveness. Proceedings of the 4th Multidisciplinary International Social Networks Conference on ZZZ - MISNC '17. https://doi.org/10.1145/3092090.3092114
[50] Van Osch, W. et al. (2015). Enterprise social media: Challenges and opportunities for organizational communication and collaboration. 2015 48th Hawaii International Conference on System Sciences. https://doi.org/10.1109/hicss.2015.97
[51] Pasquini, C. et al. (2021). Media forensics on social media platforms: A survey. EURASIP Journal on Information Security, 2021(1). https://doi.org/10.1186/s13635-021-00117-2
[52] Reuber, A. R., & Fischer, E. (2021). Annual review article: Relying on the engagement of others: A review of the governance choices facing social media platform start-ups. International Small Business Journal: Researching Entrepreneurship. https://doi.org/10.1177/02662426211050509
[53] Schoenebeck, S., & Blackwell, L. (2021). Reimagining social media governance: Harm, accountability, and repair. SSRN Electronic Journal. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3895779
[54] Schoenebeck, S., & Blackwell, L. (2021). Reimagining social media governance: Harm, accountability, and repair. SSRN Electronic Journal. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3895779
[55] Kumar, S., & Alok Nikhil Jha. (2022). Fake news goes viral! Determination and analysis of virality of socially relevant events in digital governance. https://doi.org/10.1145/3560107.3560165
[56] Costello, C. et al. (2016). Adolescents and social media: Privacy, brain development, and the law. web.archive.org/web/20200321095330id_/jaapl.org/content/jaapl/44/3/313.full.pdf
[57] Mkhize, S. et al. (2020). An examination of social media as a platform for cyber-violence against the LGBT+ population. Agenda, 34(1), 23-33. https://doi.org/10.1080/10130950.2019.1704485
[58] Vrhovec, S., & Fujs, D. (2023). Are perceptions about government and social media providers related to protection motivation online? International Journal of Cyber Behavior, Psychology, and Learning, 13(1), 1-19. https://doi.org/10.4018/ijcbpl.324085
[59] Garon, J. (2013). Social media in the workplace from constitutional to intellectual property rights. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2348779
[60] Wang, Y., & Gray, J. E. (2022). China's evolving stance against tech monopolies: A moment of international alignment in an era of digital sovereignty. Media International Australia. https://doi.org/10.1177/1329878x221105124