ASSESSING PRIVACY CONCERNS IN SOCIAL MEDIA: A COMPREHENSIVE STUDY OF MEASUREMENT SCALES AND FRAMEWORKS

Hashim H Puthiyakath, PhD Student, Department of Media and Communication, Central University of Tamil Nadu, Thiruvarur, India
Dr Manash P Goswami, Associate Professor, Department of Media and Communication, Central University of Tamil Nadu, Thiruvarur, India,
Email: mpgoswami@gmail.com, phone: +919999915977

Abstract

This paper examines the evolution of privacy concern scales, focusing on their application in social media. Over time, these scales have developed from broad internet privacy to more context-specific measurements like social media privacy. Key trends identified include the multidimensional nature of privacy, increased emphasis on perceived control over personal data, and the inclusion of social threats within privacy concerns. Despite their evolution, gaps still exist, particularly in capturing the nuances of social media and emerging technologies. The paper concludes with recommendations for developing more nuanced, context-specific, and comprehensive privacy concern scales to better navigate the complexities of privacy in the evolving digital world. This study contributes to understanding privacy in digital spaces and aids the creation of more effective privacy concern scales in the future.

Keywords: privacy concern scales, multidimensional privacy, social media privacy concern, online privacy concern

Introduction

The advent and evolution of social media platforms have reshaped how we communicate, socialise, and share personal information. While these platforms offer countless benefits, they simultaneously expose users to privacy concerns, increasing anxieties about personal information misuse, unauthorised data access, and potential identity theft. As such, assessing privacy concerns in social media has become a salient issue for researchers, policymakers, and platform designers alike.

Privacy concerns refer to individuals' apprehensions about losing control over personal information, causing them to be cautious about their online activities and interactions. Given the diversity in user behaviours and attitudes towards privacy across various social media platforms, accurately measuring and understanding these concerns becomes a complex task. Several scales and frameworks have been formulated and implemented to tackle this complexity in academic and industrial research. However, a comprehensive review of these existing scales and frameworks, including their strengths, weaknesses, and applicability, is currently lacking in the literature. As privacy concerns continue to evolve with technological advancements and changes in social media usage patterns, it is crucial to reassess these tools for their relevance and effectiveness in the present scenario.

This paper aims to provide an extensive examination of the scales and frameworks used to measure privacy concerns in social media. This study will critically examine these tools by

comparing their theoretical grounding, psychometric properties, and practical implications. By identifying potential gaps and shortcomings, the study is expected to illuminate improvement areas and suggest future research directions.

Theoretical Background on Privacy Concerns

Understanding the theoretical background of privacy concerns is fundamental to fully comprehending the significance and nuances of the measurement scales and frameworks used in the context of social media. Privacy concerns refer to individuals' apprehensions about losing control over personal information, and such concerns have become more prominent with the advent of social media platforms where personal information is shared widely and often.

The concept of privacy has been discussed and studied across various disciplines, including psychology, sociology, information systems, and law, leading to a multitude of theoretical perspectives. A fundamental distinction in these perspectives can be drawn between normative theories, which often frame privacy as a rights-based concept, and descriptive theories, which view privacy as a finite resource that may diminish until it is ultimately forfeited (Tavani, 2007).

The most fundamental perspective regarding privacy as a right is attributed to Westin (1968), whose definition posits privacy as the individuals' entitlement to govern the dissemination of information about themselves to others. This notion of privacy as control over personal information remains highly influential and forms the backbone of many privacy scales and frameworks. It corresponds to the interpretation of privacy that emphasizes the avoidance of intrusion and the ability to maintain personal boundaries, drawing upon an understanding of privacy in relation to spatial contexts (Altman, 1975).

With the emergence of the internet and digital platforms, the spatial perspective of privacy has undergone transformation. Specifically, there has been a shift in focus from a spatial understanding of privacy to a greater emphasis on information privacy. Nevertheless, similarities persist between these interpretations, particularly in terms of the significance placed on regulating or controlling access to the self (Margulis, 2003). Information privacy is often perceived as limiting access to personal information or as the autonomy that individuals possess over information pertaining to themselves (Tavani, 2007).

While privacy as a concept has always been of importance, the advent of the internet and subsequent digital platforms, especially social media, has brought privacy concerns to the forefront of discourse. It has become imperative to articulate, measure, and address these concerns in these new contexts. Accordingly, theoretical perspectives evolved, adapting to the unique challenges posed by the digital age, thus forming the foundation of privacy apprehensions in the realm of the internet. More recent approaches have re-examined the concept of privacy highlighting the distinction between "privacy as hiding" (confidentiality), "privacy as control" (informational self-determination), and "privacy as practice" (identity construction) (Berendt, 2012; Gürses, 2010). Among these, the last two concepts encompass the individual's effective ability to actively shape their identity by strategically disclosing or

concealing data, as well as actively engaging in the management of existing data flows and renegotiating social boundaries regarding collected data. This perspective on privacy as practice is especially relevant in the context of social media, where users continually navigate the boundary between sharing personal information for social interaction and preserving their privacy. For example, Smith et al. (1996) introduced the four dimensions of privacy concerns in the Internet context, which have been widely adopted in the social media context as well: collection, unauthorised access, secondary use, and errors. 'Collection' refers to concerns about the amount of personal information collected and the belief that it is excessive. 'Unauthorized access' refers to concerns about improper or unauthorised access to personal information. 'Secondary use' refers to concerns that information is used for purposes other than those for which it was initially collected. 'Errors' refer to concerns about inaccuracies in personal data and difficulties in correcting them.

Another significant theoretical perspective is offered by Petronio's (2002) communication privacy management (CPM) theory. This theory posits that people perceive their personal information as something they own and thus have the right to control. They set up privacy boundaries that dictate the rules of sharing this information. Privacy turbulence occurs when these rules are violated, for instance, when personal information shared on social media is disseminated without consent. This perspective offers a comprehensive understanding of privacy concerns, especially as it emphasises the dynamic nature of privacy management in social media.

From an information systems perspective, privacy concerns are often studied through the lens of the privacy calculus theory (Dinev&Hart, 2006). This theory suggests that individuals make a trade-off between the potential advantages they can get by disclosing personal information and the potential risks of such disclosure. In the context of social media, the benefits might include social interaction and information sharing, while the risks are related to privacy loss and misuse of personal information.

Understanding privacy from a cultural perspective is also important. Hofstede's (1980) cultural dimensions theory suggests that people's behaviour, including their privacy concerns, is significantly influenced by the culture they belong to. For example, individuals in collectivist cultures might have different privacy concerns compared to those in individualist cultures. Understanding these cultural nuances is crucial for developing and adapting privacy concern scales and frameworks.

The legal perspective on privacy is also vital, with the fundamental principle that privacy is a human right, as asserted by the Universal Declaration of Human Rights. This has prompted the formulation and implementation of privacy laws and regulations in many countries. However, the constant evolution of technology, including social media platforms, often outpaces the development of privacy laws, leading to gaps that might heighten privacy concerns.

Measuring privacy concern

Due to several key factors, understanding and assessing privacy concerns on social media platforms has become a critical area of focus.

Firstly, Privacy concerns can act as a significant determinant for an individual's decisions regarding joining, using, and interacting on a social media platform. They may influence the extent of personal information disclosure, the level of engagement with various platform features, and the adoption of privacy-protective measures. For instance, individuals with heightened privacy concerns might choose to limit their activity on the platform or utilise privacy settings more effectively to manage their information disclosure.

Secondly, assessing privacy concerns is a critical factor in exploring and untangling the so-called privacy paradox. This paradox reflects the observed incongruity where users' expressed privacy concerns do not align with their actual disclosure behaviours on social media. A systematic measure of privacy concerns provides a more nuanced understanding of this paradox, informing potential strategies to mitigate this divergence between user concerns and behaviours.

Lastly, by offering insights into users' privacy attitudes and concerns, these measures can guide the design and policies of social media platforms. Design approaches that prioritize the user, guided by an understanding of privacy concerns, can facilitate the creation of features and services that are more attuned to privacy considerations. Similarly, insights into privacy concerns can inform the formulation of more effective and user-friendly privacy policies, which are critical in establishing users' trust in the platform. Moreover, a comprehensive understanding of privacy concerns can aid in creating targeted user education programs, enhancing users' awareness and knowledge about privacy risks and protective measures.

In essence, the measurement of privacy concerns is more than just of academic interest. However, it carries substantial implications for the broader digital ecosystem, including users, social media platforms, policymakers, and society at large.

Approaches to measuring privacy concern

Survey methodologies for measuring privacy concerns typically employ one of three main approaches, each capturing unique facets of this complex construct:

1. Direct Measurement Approach: The direct measurement approach is perhaps the most straightforward means of measuring privacy concerns. This method involves directly asking respondents to indicate their level of concern about privacy. While this approach may not capture the full complexity of privacy concerns, it offers a quick and straightforward method of gauging general privacy attitudes.
2. Scenario-Based Approach: This approach takes into account the context-specific nature of privacy concerns by presenting respondents with specific scenarios involving potential privacy invasions. For example, a scenario might describe a situation where a social media platform shares user data with third-party advertisers.

Participants are then requested to rate their degree of privacy concern in each given scenario. This method aims to approximate real-world situations and can provide a more practical and contextualised assessment of privacy concerns.

3. Latent Variable Approach - Indirect Measurement through Concerns about Practices: In this approach, privacy concern is assumed to be a latent variable that is not measured directly. Instead, respondents are asked about their level of concern regarding certain practices that could potentially invade their privacy. For example, they might be asked to rate their concern about social media platforms tracking their online activities or sharing their data without their explicit consent. The responses to these questions are then used to infer the underlying level of privacy concern.
4. Latent Variable Approach - Indirect Measurement through Privacy-Enhancing Behaviours: This approach also treats privacy concern as a latent variable, but it measures this indirectly through individuals' engagement in privacy-enhancing behaviours. Respondents might be asked to rate how often they engage in behaviours like changing their privacy settings, using anonymous browsing modes, or deleting cookies. These behaviours are used as indicators of underlying privacy concerns, offering an indirect yet practical measure of privacy attitudes.

A considerable number of studies investigating privacy concerns employ ad-hoc questionnaires tailored explicitly to the context of their research. Although these tools offer flexibility, they may lack consistency and comparability across different studies since their reliability and validity often remain unverified. However, in the landscape of privacy research, there are indeed validated scales designed to measure privacy concerns. However, these rigorously validated scales are relatively scarce.Given the increasing significance of privacy concerns within the realm of social media usage, the need for such robust measures becomes increasingly urgent. Consequently, this review is designed to address this gap, comprehensively examining existing validated scales for measuring privacy concerns in social media settings.

Methodology

This review adopts a narrative literature review approach, focusing on examining and comparing measurement scales and frameworks used to assess privacy concerns in social media.

Search Strategy

The literature search aimed to identify articles that proposed or utilised unique scales or frameworks for measuring privacy concerns in social media. The search was conducted on two major academic databases for social sciences: Scopus and Web of Science. The search was designed with a combination of keywords "privacy concern(s)", "social media", "measurement", "scale(s)", "framework(s)", "model(s)", and "tool(s)". The search was restricted to articles written in English and published until June 2023.

Inclusion and Exclusion Criteria

Criteria for inclusion encompassed articles that proposed a new scale or framework for measuring privacy concerns in social media or those that employed a unique scale or framework for such assessments. Exclusion criteria were non-English articles, studies not focused on social media, articles without a precise scale or framework, and non-peer-reviewed articles.

Study Selection and Data Extraction

Following the search process, a compilation of citations was created, and duplicates were eliminated. Subsequently, the titles and abstracts underwent a comprehensive evaluation, adhering to predetermined inclusion criteria. The full texts of potentially eligible studies were meticulously assessed to determine their appropriateness for inclusion in the analysis. Information pertaining to each identified scale or framework, such as authors, year of publication, privacy concern definition, captured dimensions of privacy concern, and the number of items, was extracted.

Quality Assessment and Data Synthesis

The quality of each scale or framework was evaluated based on reliability, validity, comprehensiveness, and clarity of construction and scoring. Data were synthesised narratively due to the anticipated heterogeneity of the scales and frameworks, and a comparative table was constructed.

This methodology ensures a thorough review of the scales and frameworks for assessing privacy concerns in social media, providing a valuable resource for researchers and practitioners. Furthermore, this analysis identifies noteworthy gaps in the existing research and presents potential opportunities for future investigations in this field.

A Critical Review of Validated Scales for Measuring Privacy Concerns in Social Media

Although various scales have been employed to measure these concerns, there are relatively few validated and standardised instruments specific to the social media context. This section presents a comprehensive review of validated scales explicitly designed to measure privacy concerns in the realm of social media. Each scale is critically evaluated in terms of its theoretical underpinnings, psychometric properties, and applicability in different social media contexts. The goal is to guide future researchers and practitioners in selecting the most suitable tool for their studies and interventions, thereby promoting consistency and rigour in privacy-concern research.

Concern for Information Privacy (CFIP) Scale by Smith et al. (1996)

The Privacy Concern Scale, developed by Smith, Milberg, and Burke (1996), came about to meet the demand for a systematic tool that could gauge individuals' concerns about organisational privacy practices in a consumer context. Rooted in the notion of privacy as a

multidimensional construct, the scale comprises 15 items measuring four dimensions of privacy concerns: Collection, Unauthorized secondary use, Errors, and Improper access. Respondents are required to evaluate each item on a 7-point Likert scale.

With high Cronbach's alpha values (.88 for Collection, .84 for Errors, .80 for Secondary Use, and .75 for Improper Access), the scale's internal consistency was notable. The scale also had a Root Mean Squared Residual of 0.065, indicating a good fit. Furthermore, the scale exhibited satisfactory convergent and discriminant validity and nomological validity, underscoring its overall reliability and applicability for privacy concern research.

Since its creation, it has found extensive application in privacy research, specifically in consumer behaviour and e-commerce fields.

A key strength of this scale is its multidimensional character and robust psychometric properties. However, as it predates the advent of social media, it might not wholly encompass privacy concerns particular to social media. Even though it was not designed with social media in mind, it has been adapted for such contexts in numerous studies. However, alterations may be necessary to ensure its relevance for capturing privacy concerns related to contemporary social media usage.

In summary, this scale is well-suited to studies that require a comprehensive understanding about the privacy apprehensions. However, the scale requires modifications, followed by a reassessment of its reliability and validity to ensure that it appropriately gauges privacy concerns in the realm of online social networking sites.

Internet Users Information Privacy Concern Scale (IUIPC) by Malhotra et al. (2004)

Developed by Malhotra et al. (2004), the Internet Users' Information Privacy Concerns (IUIPC) Scale has been instrumental in assessing individuals' apprehensions regarding collection, unauthorised secondary use, and control over the personal data online. Guided by the social contract theory of privacy, this scale contains 10 items distributed across three dimensions - Collection, Secondary use, and Control, with responses solicited on a 7-point Likert scale.

The IUIPC demonstrates excellent psychometric properties, as evidenced by the Composite Reliability (CR) values ranging from 0.74 to 0.95 and Average Variance Extracted (AVE) values ranging from 0.50 to 0.86, both surpassing the recommended thresholds. Convergent and discriminant validity are established, and the scale effectively captures the overall construct of privacy concerns among internet users. However, it is worth noting that the treatment of privacy concern as a higher-order construct is subject to debate.

The IUIPC has been widely used to investigate privacy concerns related to online activities such as e-commerce and social media use. It contributes significantly to understanding the factors that influence privacy apprehensions and their subsequent effect on user behaviour. A noteworthy advantage of the IUIPC is its multidimensional structure allowing the exploration of different aspects of privacy concern.

Conversely, the scale's age and primary focus on the online context might limit its comprehensiveness and applicability. Although it has been used to study privacy concerns in offline scenarios, it was principally designed for the online context.

Researchers should consider utilising the IUIPC to investigate privacy concerns online. Nonetheless, its application to different research contexts requires careful deliberation, and potential modifications may be warranted to ensure its relevance to the specific research scenario.

Internet Privacy Concerns Scale by Dinev and Hart 2004

Building upon the foundation laid by Smith et al. (1996), Dinev and Hart (2004) modified the existing scale to reflect the unique characteristics of the Internet, introducing a specific focus on privacy concerns. They successfully eliminated unrelated aspects like organisational policies and general computer anxiety, thereby producing a more concentrated measure of privacy concerns.

Their model encompassed two distinct dimensions of privacy concern: Abuse and Finding, consisting of four and ten items, respectively. Dinev and Hart's scale boasts impressive psychometric properties, with Cronbach's alpha standing at 0.9 for Abuse and 0.94 for Finding, indicating robust internal consistency. The scale also establishes sound convergent, discriminant, and predictive validity, making it a reliable measure in privacy research.

This scale was explicitly tailored to scrutinise privacy concerns in an Internet context, emphasising individuals' perceived control over their information and perceived vulnerability during online activities. Consequently, this scale has found valuable application in areas such as e-commerce, online banking, social media, and other digital platforms where privacy concerns have relevance.

The instrument is well-suited for studies seeking to dissect and comprehend the attitudes and concerns of individuals regarding their privacy while using the Internet. However, the specific, context-driven design of this scale can also be perceived as a limitation, as it may not capture the full breadth of privacy concerns. Moreover, the two-dimensional structure of the scale may fall short in accounting for all facets of privacy concern, given the complex, multi-dimensional nature of the construct. This suggests that although the scale offers a targeted tool for examining social media privacy concerns, its scope and application may be restricted in some respects.

Online Privacy Concern Scale by Buchanan et al. (2007)

Buchanan et al. (2007) initially sought to capture multiple dimensions of privacy concern in their instrument development, consistent with the multifaceted nature of privacy outlined by previous research. Unexpectedly, their analysis revealed a single interpretable attitudinal factor, leading to a unidimensional representation of privacy concern in their study. This construct, although limited in its multifactorial representation, nevertheless provides an

improvement over prior brief measures by tapping into several aspects of privacy. These aspects include accessibility, informational privacy, and expressive privacy.

Importantly, unlike several other scales, Buchanan et al.'s scale has been demonstrated to be valid online environments. This strengthens the efficiency of the instrument but it should be noted that it treats privacy concern as a single composite score rather than having individual sub-constructs for the various theoretically delineated aspects of privacy. Essentially, the scale's unidimensional nature may limit the depth of understanding it can provide into the multi-layered privacy concerns experienced by users in various digital contexts, particularly on online social networking platforms where privacy dynamics are overly intricate.

With regard to psychometric properties, Buchanan et al.'s scale displayed adequate reliability and validity, making it a robust tool for the measurement of general privacy concerns. However, researchers should exercise caution when utilising this scale in studies where a more granular understanding of privacy concerns is required, given its unidimensional nature.

Internet Privacy Concerns Scale by Hong and Thong (2013)

The Internet Privacy Concerns (IPC) scale, developed by Hong and Thong in 2013, builds upon established instruments, including those from Smith et al. (1996) and Malhotra et al. (2004), to meet the growing need for a comprehensive tool measuring contemporary perceptions of online information privacy. This scale consists of six key dimensions: collection, secondary usage, errors, improper access, control, and awareness, with respondents rating each item on a Likert scale.

The IPC scale is notable for its third-order factor structure, which consistently outperformed corresponding lower-order factor models in their study, demonstrating strong internal consistency and construct validity. It has been widely used in privacy research, particularly in studies of online consumer behaviour and e-commerce, and has significantly contributed to understanding privacy concerns.

One of the IPC scale's primary strengths is its multidimensional nature, enabling researchers to capture a wide range of privacy concerns. However, its third-order factors can be challenging to implement in some contexts. The scale is designed explicitlyto study privacy concerns in online environments like e-commerce, social media, and other online platforms. Therefore, while it is ideal for studies focusing on the flow and management of personal information online, adaptation may be needed for other contexts.

In conclusion, the IPC scale is a valuable tool for comprehensive online privacy research, particularly for studies examining the intricacies of personal information management online. As with any scale, researchers are advised to confirm its reliability and validity within their specific context.

The Privacy Concerns in Online Social Networking (PCOSN) scale by Krasnova et al. (2009)

The Privacy Concerns in Online Social Networking (PCOSN) scale developed by Krasnova et al. (2009)was specifically designed to measure user privacy concerns in therealmof Online Social Networks (OSNs). Developed through a multi-stage process that included focus group discussions and questionnaire development, the scale uniquely captures the dual dimensions of privacy concerns: Organizational Threats and Social Threats.

The “Concerns about Organizational Threats” dimension encapsulates user worries regarding the gathering, storage, and utilisation of their information by OSN providers and third parties. Interestingly, the researchers found that users do not usually differentiate between the entities collecting and using their information or between the processes of data collection and secondary use. On the other hand, the “Concerns about Social Threats” dimension relates to apprehensions about risks within the OSN user environment. It encompasses various concerns related to interactions with other users, such as cyberbullying, harassment, privacy breaches, identity theft, exposure to inappropriate or harmful content, and the potential impact on one's reputation or social relationships.

The psychometric properties of the scale indicate its robustness, with Composite Reliability values surpassing the threshold of 0.6 and Average Variance Extracted (AVE) values reaching or exceeding the threshold level of 0.5. Additionally, the scale demonstrates discriminant validity, as evidenced by the square root of the AVE for each latent variable being greater than the correlation between that variable and any other latent variables. These findings affirm the reliability and validity of the scale for measuring the intended constructs.

The PCOSN scale has proven valuable in analysing the impactof privacy apprehensions on user behaviour in OSNs. For instance, the study found that concerns about organisational threats negatively influenced the amount of information users disclosed on OSNs, whereas concerns regarding social threats impacted the honesty and deliberate control of information disclosure.

Although this scale provides an essential tool for examining privacy concerns in OSNs, its limitations should be considered. It is noteworthy that the dimensions of "Accessibility Threats" and "Identity Theft", despite being significant in focus group discussions, did not emerge as separate factors in the scale. It suggests that the scale may not cover all possible dimensions of privacy concerns in the realm of online social networking sites.

The PCOSN scale provides a valuable tool for research aimed at understanding privacy concerns in the social networking context. Its focus on both organizational and social threats allows for a comprehensive understanding of users' concerns, which can influence the amount, honesty, and control of information individuals disclose on OSNs.

Li and Wang (2022)

Li and Wang (2022) developed a new scale specifically for assessing privacy concerns in the realm of social media, building on the foundational work of Malhotra et al. (2004). The scale enriches understanding of privacy concerns in the social media sphere, featuring four dimensions: collection, control, perception, and secondary usage.

The researchers devised the User Privacy Concern Measurement Scale using the Internet User Information Privacy Concern Scale (IUIPC) from Malhotra et al. (2004) as a basis. The original IUIPC scale covered three elements: collection, control, and awareness. Li and Wang, however, introduced a "secondary use" dimension to better encapsulate privacy concerns within the social media realm. Following an exploratory factor analysis of the questionnaire items, they finalised four dimensions and twelve items for the scale. This scale then underwent adjustment and validation through large sample testing.

The reliability and validity of the User Privacy Concern Measurement Scale are reported to be strong. With Cronbach's α coefficients for all four dimensions exceeding 0.8, the scale demonstrates good reliability. The scale's explanatory power is relatively robust at 77.746%, indicating its efficacy in measuring privacy apprehensions with regard to online social networking sites.

Despite its strengths, the scale also presents potential drawbacks. A primary concern is the 'perception' dimension's overlap with the 'control' dimension, which could lead to redundancy. Moreover, the scale does not explicitly address direct privacy threats such as unauthorised access or identity theft, significant concerns within the social media context. Furthermore, it does not take into account social aspects of privacy concerns in online social networking sites, such as invasions of privacy from other users or concerns related to user-generated content. As such, while providing a nuanced perspective on privacy concerns in the social media context, this scale may require additional measures or modifications to capture a more comprehensive picture of privacy concerns in online social networks.

Discussion

Upon detailed review of the aforementioned privacy concern scales, it is clear that these tools have evolved over time to capture the changing nature and context of privacy concerns, particularly in the realm of social media. This evolution has been dictated by a host of factors, ranging from technological advancements and increased online engagement to changing societal norms and legal regulations regarding privacy. Each scale has a unique perspective and theoretical underpinning, providing researchers with a broad spectrum of tools to measure and investigate privacy concerns.

A common thread across these scales is their reliance on the multidimensional construct of privacy. Starting from the seminal work of Smith et al. (1996), most scales have embraced the notion that privacy concerns are not a unidimensional construct but rather composed of several distinct yet related dimensions. These can include aspects like collection, control, secondary use, and awareness, amongst others. This multidimensionality allows for a more

granular and comprehensive understanding of privacy concerns, capturing the complexity and diversity of user apprehensions in the digital space.

A significant shift in the development of these scales is the transition from a broad focus on internet privacy concerns to more specific contexts like e-commerce or social media. The scales of Malhotra et al. (2004), Dinev and Hart (2004), and Hong and Thong (2013) expanded upon Smith et al.'s (1996) scale to reflect the unique characteristics of the Internet and e-commerce. However, the focus of these scales remained broad. The scales developed by Krasnova et al. (2009) and Li and Wang (2022) are designed specifically for social media, indicating a trend toward context-specific privacy concern scales.

This trend towards specificity is a response to the increasing complexity of the digital landscape. As users interact with various platforms, their privacy concerns can differ significantly based on the platform's characteristics, the type of data involved, and the potential uses of that data. Hence, scales tailored to specific contexts like social media are becoming increasingly relevant.

Another notable trend is the inclusion of perceived control as a key dimension of privacy concerns. Scales like those developed by Malhotra et al. (2004), Dinev and Hart (2004), Hong and Thong (2013), and Li and Wang (2022) consider perceived control over personal information as a significant factor influencing privacy concerns. This emphasis suggests a growing recognition of the importance of user agency and autonomy in privacy discourse.

The inclusion of social threats, as seen in Krasnova et al.'s (2009) PCOSN scale, is a unique and important development in understanding privacy concerns in social media. This highlights the growing recognition of social privacy threats arising from other users in the network, reflecting the interactive nature of social media platforms. This trend might pave the way for more nuanced studies investigating the interplay between privacy concerns, social interactions, and user behaviour on social media platforms.

Finally, using psychometric properties to validate these scales is a constant across all instruments. Robust testing of reliability and validity has lent credibility to these scales and facilitated their wide application across various studies. This practice is likely to persist as new scales are developed and old ones refined.

While these trends showcase the evolution of privacy concern scales, they also highlight existing gaps. Scales need to capture better the nuanced dynamics of social media, including aspects like user-generated content, interactions with other users, and the unique features of different social media platforms. Furthermore, scales should take into account new privacy threats and issues arising from the ever-evolving technology landscape, including aspects like AI, machine learning, and big data analytics. Future scales might also benefit from incorporating the impact of cultural, societal, and individual factors on privacy concerns.

Overall, the landscape of privacy concern scales is dynamic, with each scale reflecting the privacy discourse and concerns of its time. Future scales will likely continue this trend,

evolving to capture the changing nature and context of privacy concerns, particularly in the age of social media.

Conclusion

Privacy concern scales serve as essential tools for discerning individuals' perceptions, interpretations, and responses to privacy threats in the digital landscape, specifically within social media. As these scales have evolved over time, they have adapted to capture the shifting context and nature of privacy concerns. Even with such advancements, gaps persist in comprehending privacy concerns, especially within the social media environment. As the digital landscape is in constant flux, it is imperative that the tools employed to study it adapt accordingly. By adhering to the recommendations presented in this review, the development of more nuanced, context-specific, and comprehensive privacy concern scales can be facilitated. These scales, reflecting the multifaceted nature of privacy in the digital age, will be instrumental in continually navigating the complexities of privacy in an unceasingly evolving digital world.

References

1. Tavani, H. T. (2007). PHILOSOPHICAL THEORIES OF PRIVACY: IMPLICATIONS FOR AN ADEQUATE ONLINE PRIVACY POLICY. Metaphilosophy, 38(1), 1–22. https://doi.org/10.1111/j.1467-9973.2006.00474.x
2. Westin, A. F. (1968). Privacy And Freedom. Washington and Lee University School of Law Scholarly Commons. https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20/
3. Altman, I. (1975). The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding. Monterey, Calif. : Brooks/Cole Publishing Company.
4. Margulis, S. T. (2003). Privacy as a Social Issue and Behavioral Concept. Journal of Social Issues, 59(2), 243–261. https://doi.org/10.1111/1540-4560.00063
5. Berendt, B. (2012). More than modelling and hiding: towards a comprehensive view of Web mining and privacy. Data Mining and Knowledge Discovery, 24(3), 697–737. https://doi.org/10.1007/s10618-012-0254-1
6. Gürses, S. (2010). PETs and their users: a critical review of the potentials and limitations of the privacy as confidentiality paradigm. Identity in the Information Society, 3, 539–563. https://doi.org/10.1007/s12394-010-0073-8
7. Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. Management Information Systems Quarterly, 20(2), 167. https://doi.org/10.2307/249477
8. Petronio, S. (2002). Boundaries of Privacy: Dialectics of Disclosure. SUNY Press.
9. Dinev, T., & Hart, P. '. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. Information Systems Research, 17(1), 61–80. https://doi.org/10.1287/isre.1060.0080
10. Hofstede, G. (1980). Culture and Organizations. International Studies of Management and Organization, 10(4), 15–41. https://doi.org/10.1080/00208825.1980.11656300
11. Malhotra, N. K., Kim, S. W., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research, 15(4), 336–355. https://doi.org/10.1287/isre.1040.0032
12. Dinev, T., & Hart, P. '. (2004). Internet privacy concerns and their antecedents - measurement validity and a regression model. Behaviour & Information Technology, 23(6), 413–422. https://doi.org/10.1080/01449290410001715723

13. Buchanan, T. A., Paine, C., Joinson, A., &Reips, U. (2006). Development of measures of online privacy concern and protection for use on the Internet. Journal of the Association for Information Science and Technology, 58(2), 157–165. https://doi.org/10.1002/asi.20459
14. Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. Mis Quarterly, 275-298. https://www.jstor.org/stable/43825946
15. Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. Identity in the Information Society, 2(1), 39–63. https://doi.org/10.1007/s12394-009-0019-1
16. Li, C., Wang, C., & Chau, P. Y. K. (2022). Revealing the black box: Understanding how prior self-disclosure affects privacy concern in the on-demand services. International Journal of Information Management, 67, 102547. https://doi.org/10.1016/j.ijinfomgt.2022.102547
17. Li, R., & Wang, Y. (2022). Development and Construction of a User Privacy Concern Measurement Scale in Social Media. In Proceedings of the 2022 6th International Seminar on Education, Management and Social Sciences (ISEMSS 2022) (pp. 212–221). https://doi.org/10.2991/978-2-494069-31-2_26