Privacy Concerns and Self-disclosure in Private and Public Uses of Social Media

Anatoliy Gruzd, PhD[1] and Ángel Hernández García, PhD[2]

Keywords: social media, privacy paradox, private vs public, information privacy, self-disclosure

[1] gruzd@ryerson.ca Ted Rogers School of Management, Ryerson University, Toronto, Canada.
[2] angel.hernandez@upm.es Department of Organization Engineering, Business Administration and Statistics, Universidad Politécnica de Madrid, Madrid, Spain.

Abstract

The study contributes to the ongoing debate about the ‘privacy paradox’ in the context of using social media. The presence of a privacy paradox is often declared if there is no relationship between users’ information privacy concerns and their online self-disclosure. However, prior research has produced conflicting results. The novel contribution of this study is that we consider public and private self-disclosure separately. The data came from a cross-national survey of 1,500 Canadians. For the purposes of the study, we only examined the subset of the 545 people who had at least one public account and one private account. Going beyond a single view of self-disclosure, we captured five dimensions of self-disclosure: Amount, Depth, Polarity, Accuracy, and Intent; and two aspects of privacy concerns: concerns about organizational and social threats. To examine the collected data, we used Partial Least Squares Structural Equation Modeling (PLS-SEM). Our research does not support the presence of a privacy paradox as we found a relationship between privacy concerns from organizational and social threats and most of the dimensions of self-disclosure (even if the relationship was weak). There was no difference between patterns of self-disclosure on private versus public accounts. Different privacy concerns may trigger different privacy protection responses and, thus, may interact with self-disclosure differently. Concerns about organizational threats increase awareness and accuracy while reducing amount and depth, while concerns about social threats reduce accuracy and awareness while increasing amount and depth.

Introduction

Considering the prevalence of self-disclosure on social media, research has sought to understand what makes one to divulge personal information online by examining a number of intrinsic and extrinsic factors[1]. One such factor is a concern about individual privacy. Understanding how one's privacy concerns may influence their self-disclosure on social media is especially relevant today, in light of a recent scandal of Cambridge Analytica misusing data from millions of Facebook users to improve micro-targeting in political ads, and a consequent user-driven #DeleteFacebook campaign[2,3]. According to Privacy Calculus Theory (PCT), people make conscious decisions about their self-disclosure by weighing the benefits of disclosure against their privacy concerns associated with such disclosure[4]. The theory contends that people with increased privacy concerns would share less on social media; nonetheless, privacy concerns alone may not stop people from self-disclosing since either their perceived benefits outweigh the perceived risks, or their privacy concerns are being moderated by information privacy protection strategies[5–8].

We contribute to this research in the following three ways. First, the self-disclosure construct often used in privacy and self-disclosure research mostly captures depth and/or breadth of disclosure, while omitting other dimensions of self-disclosure[9]: accuracy, intention and polarity. Second, privacy concerns are often examined without separating organizational and social threats (with few exceptions[10,11]). We examine the relationship between privacy concerns and self-disclosure using all five dimensions of self-disclosure and two separate constructs of privacy. The distinction recognizes that social media users may be concerned about data misuse by organizations or other social media users. Thus, we ask:

> RQ1: Is there a relationship between organizational privacy concerns and self-disclosure on social media?

RQ2: Is there a relationship between concerns about social threats and self-disclosure on social media?

Third, prior research often asks respondents about social media use without indicating whether the disclosure occurs on private or public accounts; as a result, we ask respondents to report their disclosure in accordance with their own privacy boundaries and report whether their accounts are primarily private or primarily public. This is an important distinction as the notions of 'private' and 'public' are not binary, but contextual and user-specific[12–14]. Furthermore, even within a single platform there may be different levels and expectations of privacy[15,16]. To understand the role of public and private uses of social media, we ask:

RQ3: If there is a relationship between organizational privacy and social threats concerns and self-disclosure, are these relationships contingent on the type of social media account (private versus public)?

Literature Review and Hypotheses

To understand what influences people's privacy concerns and inform organizations how they can minimize risks and reduce negative perception, scholars have examined factors contributing to people's concerns associated with information privacy. Smith, Milberg, and Burke's Concern for Information Privacy (CFIP)[17] identified four fundamental factors that influence privacy concerns in response to organizations' use or potential use of personal information: collection, unauthorized secondary use, improper access, and errors in personal information. Stewart and Segars refined CFIP as a multidimensional construct comprising the four variables[18]. CFIP has been validated in various contexts such as internet use[19], mobile use[20], m-commerce[21], and instant messaging[22]. By applying CFIP to social media use, Osatuyi developed the Concern for Social Media Information

Privacy measurement scale (CFSMIP)[23]. In addition, Krasnova proposed the Concern about Social Threats scale (CST) to measure concerns about social threats from other users potentially misusing their information or posting embarrassing content about them[24,25].

Self-disclosure refers to a social process of sharing private information with another[9]. Although the concept originally focused on disclosure between two people, it is also useful in the context of sharing private information with more than one person on social media[26]. As proposed by Wheeless[9], self-disclosure expands across five dimensions: Intent: the disclosure is intentional or not; Amount: length and frequency of disclosure; Polarity: positive or negative valence; Depth: level of intimacy, and Accuracy: level of truthfulness. All five dimensions are important as they may be influenced by one's privacy concerns, but at different levels.

This study contributes to the ongoing debate about the 'privacy paradox'[27]. The presence of a privacy paradox is declared if there is no relationship between users' privacy concerns and their online participation[28,29]. However, prior research has produced conflicting results that may be due to different study populations, contexts, and platforms, or may be explained by the operationalization of privacy concerns and self-disclosure.

To interrogate the presence of the privacy paradox, we first turn to work on Information Privacy-Protective Responses (IPPR). When a user perceives a threat to their privacy, they engage in IPPR, which may include information provision, private action, or public action.[30] For example, a user may choose not to post information; thus, reducing the amount and depth of self-disclosure. Thus, we hypothesize:

H1a: CFSMIP negatively predicts the *amount* of self-disclosure on social media.

H1b: CST negatively predicts the *amount* of self-disclosure on social media.

H2a: CFSMIP negatively predicts the *depth* of self-disclosure on social media.

H2b: CST negatively predicts the *depth* of self-disclosure on social media.

Self-disclosure accuracy and polarity relate to how people manage their online identity. According to Leary and Kowalski's impression management work[31], people post accurate information about themselves if they feel that others may validate such information. This process has been observed in the context of online dating, as well as in a more general case of Facebook use, where users were more likely to choose not to post certain information rather than posting inaccurate information about themselves[24,32]. This may be especially applicable on social media where other users are in a position to verify one's posted information[33]. People may also recognize that third parties can use the information to make decisions about them (e.g., social media screening of job applicants[34]). Thus, we hypothesize:

H3a: CFSMIP positively predicts the *accuracy* of self-disclosure on social media.

H3b: CST positively predicts the *accuracy* of self-disclosure on social media.

People may choose to engage in "selective self-presentation"[35] to enhance their online image and present themselves in a socially desirable manner[36]. For example, Facebook users post positive emotional words in their public status updates as a strategy to manage their self-presentation on the platform[37]. In our work, we want to explore to what extent such positive self-disclosure may be linked to one's privacy concerns. Although we did not find a direct link in the literature, we hypothesize that a strategy of posting favorable content or using positive statements may be an IPPR. To test this, we pose:

H4a: CFSMIP positively predicts the positive *polarity* of self-disclosure on social media.

H4b: CST positively predicts the positive *polarity* of self-disclosure on social media.

Prior research suggests that privacy concerns have a negative relationship with intention to disclose[38,39]. However, since intent captures one's awareness of self-disclosure, this dimension is aligned with the Conscious Control construct[24], rather than the future intention to share information. Krasnova et al.[24] found that concerns about social threats made participants (primarily students) more aware of their self-disclosure in social media, but interestingly the organizational information privacy concerns did not have the same impact on self-disclosure intent (conscious control). We want to disentangle a nuanced relationship between privacy concerns and user's awareness of their self-disclosure by testing the following:

H5a: CFSMIP positively predicts the *intent* of self-disclosure on social media.

H5b: CST positively predicts the *intent* of self-disclosure on social media.

The final two hypotheses investigate the nature of self-disclosure in public or private uses of social media. Previous work[40] evidences that the perceived publicness of a social networking site has a negative relationship with the amount and depth of self-disclosure. This suggests a stronger role of privacy concerns on users' self-disclosure via public versus private accounts. Considering that social media users may share more intimate information on their private accounts that third-parties are less likely to access, we expect that concerns about threats from other users would be more pronounced than threats from third-parties when disclosing on a private account; thus, we hypothesize:

H6a: CFSMIP has a stronger impact on public self-disclosure than private self-disclosure on social media.

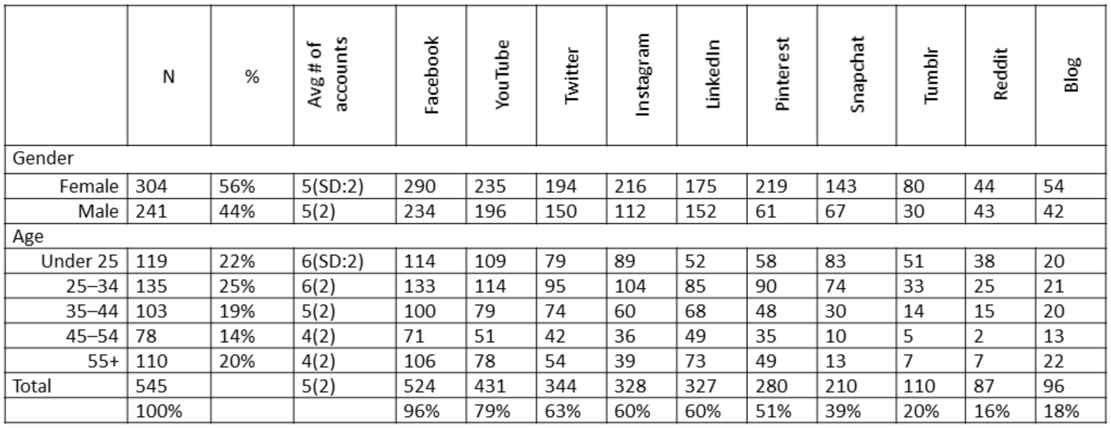
H6b: CST has a stronger impact on private self-disclosure than public self-disclosure on social media.

Method

Data collection

We collected data using a cross-national survey among Canadians based on Research Now's Internet panel population. In total, we collected 1,500 responses that were census-balanced by age, gender, and location, but in this study, we only examined the subset of the 545 people who had at least one public account and one private account (see Table 1). The online survey was open from June 1–July 15, 2017 and hosted by Qualtrics.

Table 1: Sample Demographics



	N	%	Avg # of accounts	Facebook	YouTube	Twitter	Instagram	LinkedIn	Pinterest	Snapchat	Tumblr	Reddit	Blog
Gender													
Female	304	56%	5(SD:2)	290	235	194	216	175	219	143	80	44	54
Male	241	44%	5(2)	234	196	150	112	152	61	67	30	43	42
Age													
Under 25	119	22%	6(SD:2)	114	109	79	89	52	58	83	51	38	20
25–34	135	25%	6(2)	133	114	95	104	85	90	74	33	25	21
35–44	103	19%	5(2)	100	79	74	60	68	48	30	14	15	20
45–54	78	14%	4(2)	71	51	42	36	49	35	10	5	2	13
55+	110	20%	4(2)	106	78	54	39	73	49	13	7	7	22
Total	545		5(2)	524	431	344	328	327	280	210	110	87	96
	100%			96%	79%	63%	60%	60%	51%	39%	20%	16%	18%

Instrument design

The measurement items used in this research have been validated by other researchers as outlined below (see Appendix A).

Following Lai and Yang[26], and Leung[41], we captured five dimensions of self-disclosure: Amount (SDAm), Depth (SDD), Positive/Negative Valence or Polarity (SDPN), Accuracy (SDAc), and

Intent (SDI). Originally proposed by Wheeless[9], these items have been adapted to the social media context.[41–43]

To measure privacy concerns, we relied on two constructs: concerns about social and organizational threats. Following Stewart and Segars[18], Concern for Information Privacy (CFIP) assesses concerns for information privacy in response to organizations' potential use of their personal information, across four dimensions: collection (COL), errors (ERR), secondary use (SUS), and unauthorized access (UAC). We use the CFSMIP instrument developed by Osatuyi[23]. The second privacy construct, Concern about Social Threats, represents people's concerns related to other users' potential misuse of their information. Following Krasnova et al.[24], this construct was measured using three indicators (CST1-3) related to other users posting embarrassing content or misusing information posted by this person on social media.

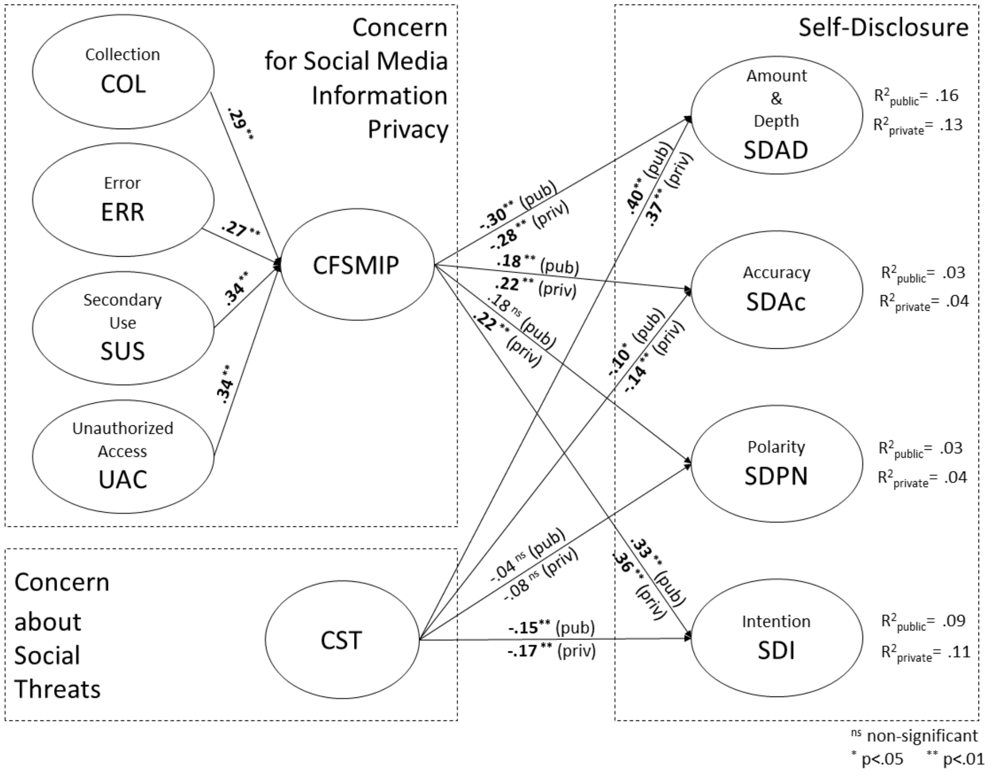
Data analysis

To examine the collected data, we used Partial Least Squares Structural Equation Modeling (PLS-SEM). PLS-SEM is the preferred method to analyze complex models when the aim of the analysis is prediction, making no assumption about data distribution[44]. Furthermore, PLS models can generate predictions and prediction intervals for manifest items both in-sample and out-of-sample[45], and perform model comparisons between two groups through multigroup analysis[46]. As there is no consistency as to whether CFIP/CFSMIP should be conceptualized as reflective-reflective or reflective-formative, we ran a confirmatory tetrad analysis, which supported the definition of the second order construct as reflective-formative. We consider a formative measurement model specification[44] as both of the measurement model's non-redundant tetrads are significantly different from zero.

We then followed a recommended two-step procedure: (1) examining reliability and validity of the measurement model and (2) analyzing the structural model[47]. We used the repeated indicators approach using a factor weighting scheme to examine the hierarchical structural model, and the bootstrapping procedure implemented in SmartPLS 3.2.6[48] with 5,000 iterations to assess the significance of paths.

The general rules for assessment follow Hair et al.[44,49]. The comparative nature of the study requires measurement model assessment and, before structural model assessment, a measurement invariance assessment. Thus, the analysis includes a measurement model assessment—of both reflective and formative variables—for each group, then a measurement invariance (configurational, compositional and scalar invariance) assessment. See Appendix B for more details. Figure 1 presents the results of the structural model assessment.

Figure 1. Results of the structural model assessment



Results

RQ1: In the context of **private** self-disclosure, CFSMIP positively predicts intent ('awareness'), polarity, and accuracy; and negatively predicts the combined dimension of amount and depth. This suggests that the *more* people are concerned about organizations collecting and using their information, the *more* they are aware of their disclosure on social media, and their disclosure tends to be more positive and accurate, while the amount and depth of disclosure is reduced. Thus, the results support hypotheses H1a–H5a in the context of private self-disclosure. A similar result emerges in the context of **public** self-disclosure: CFSMIP positively predicts intent and accuracy, and negatively predicts the combined dimension of amount and depth (Figure 1). H4a, however, is not supported as the path coefficient for polarity is not significant in the context of public self-disclosure.

RQ2: In the context of **private** self-disclosure, CST positively predicts the amount and depth of self-disclosure, and negatively predicts intent and accuracy. This suggests that the *more* people are concerned about other users misusing their social media data, the *more* they disclose online, but they are less accurate and less aware of doing so. H4b is also not supported as the path coefficient for polarity is not significant in the context of private self-disclosure. We found similar results in the context of **public** self-disclosure: CST positively predicts the amount and depth of self-disclosure, and negatively predicts intent, and accuracy. The path coefficient for polarity was not statistically significant.

These surprising results contradict H1b–3b and H5b, which suggests that concerns about social threats have an opposite relationship with self-disclosure practices compared to organizational information privacy concerns. A possible explanation is that people might be employing different IPPR depending on whether the perceived threats are from organizations or individuals. For example, users may choose to withhold information, post anonymously, share inaccurate information, or report privacy concerns to regulators[5–8]. Similarly, Alashoor et al. found a negative relationship between students' privacy concerns and their accuracy of self-disclosure in social media[50].

RQ3: Although there is one significant relationship in private networks (between organizational privacy concerns and polarity) that is not significant in public networks, the multigroup analysis evidences that there are no statistically significant differences between how and what people disclose on public and private social media accounts; therefore, we reject H6a and H6b. While some previous research identifies a negative relationship between the perceived publicness of a social media account and the amount and depth of self-disclosure[40], we found no reported difference in self-disclosure on public and private accounts. Instead, users may be developing and adopting privacy protective strategies across all of their accounts regardless of whether they are primarily public or private.

Conclusion

The study extends the privacy paradox research from studying predominately private sharing behavior to examining users' privacy expectations in the context of public sharing. Our research does not support the presence of a privacy paradox as we found a relationship between privacy concerns from organizational and social threats and most of the dimensions of self-disclosure (even if the relationship was weak). There was no difference between patterns of self-disclosure on private versus public accounts. In other words, users regulate their disclosure in accordance with their privacy concerns in a similar way, regardless of whether they share content using their private or public account. A broader implication of this finding is that even if information is publicly available on social media, users may still have expectation of privacy.

Furthermore, we found that different privacy concerns may trigger different IPPRs and, thus, may interact with self-disclosure differently. For example, concerns about organizational threats increase accuracy and awareness while reducing amount and depth, while concerns about social threats reduce accuracy and awareness while increasing amount and depth. Although the current study does not provide qualitative data to explain a peculiar relationship between social threats and the amount and depth of self-disclosure; the results broadly support the idea behind PCT that users are rational actors who recognize different privacy-related threats and also adjust what and how they share information on social media accordingly. In future work, we would like to examine how different types of heuristic rules and biases that users might have[27,51] may interact with the process of risk-benefit assessment when disclosing online.

Interestingly, we only found partial support for the idea that people are engaged in selective self-presentation[35] on social media to develop a socially desirable online identity[36]. Specifically, positive valence or polarity was only predicted by privacy concerns from organizational threats and only in the context of private accounts. This finding suggests that sharing information with positive valence is likely guided not just by the goal of selective self-presentation, but also by other reasons, such as strengthening social ties or simply expressing one's positive internal states[37,52].

From a practical perspective, organizations should recognize that social media users with both private and public accounts are concerned with all four dimensions of CFSMIP. Social media platforms that collect personal information should develop clear data stewardship policies and practices that account for people's reticence towards third-parties' unauthorized access, collection, and use of their data. If such data collection and use is happening, organizations should ensure that users' data is error free and accurate. As our research suggests, failure to address users' privacy concerns may result in users sharing less information which, in turn, may negatively impact users' overall engagement. Since our model showed there is no perceived difference in the level of self-disclosure on both public and private accounts, organizations that rely on publicly available social media data should use the same level of privacy protection and ethical consideration as if they are handling data from private accounts.

Social media platforms should also recognize that users may be concerned with the misuse of their data by other users. As our model suggests, concerns about social threats do not necessarily make people less active on social media, but they may reduce the accuracy of information shared on their public and private social media accounts. In turn, the lack of accurate information about users may reduce the usefulness of various automated recommendations and filtering features offered by most social media platforms.

From a theoretical perspective, CFSMIP and CST alone are not strong explanatory variables for some dimensions of self-disclosure; additional variables should be considered in future work. For example, we need to consider not just person-based variables (such as privacy concerns) but also demographics, system-based and environmental factors[1]. Depending on the platform and users, benefits of using social media may outweigh one's privacy concerns, as such future research can embrace a uses and gratification approach to include why people use social media[26]. Finally, as this research focused on people who have both private and public accounts, our future work will analyze the privacy concerns and self-disclosure behavior of people who only have public accounts versus those with only private accounts.

References

1. Bauer C, Schiffinger M. Self-Disclosure in Online Interaction: A Meta-analysis. In: 2015 48th Hawaii International Conference on System Sciences. ; 2015: 3621–3630.
2. Wagner K. Here's how Facebook allowed Cambridge Analytica to get data for 50 million users. Recode. Available at https://www.recode.net/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data. Accessed March 25, 2018.
3. Mack E. #DeleteFacebook trends as compromised social users fume. CNET. Available at https://www.cnet.com/news/deletefacebook-hashtag-trends-twitter-facebook-users/. Accessed March 25, 2018.
4. Culnan MJ, Armstrong PK. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organ Sci*. 1999;10:104–115.
5. Child JT, Haridakis PM, Petronio S. Blogging privacy rule orientations, privacy management, and content deletion practices: The variability of online privacy management activity at different stages of social media use. *Comput Hum Behav*. 2012;28:1859–1872.
6. Root T, McKay S. Student Awareness of the Use of Social Media Screening by Prospective Employers. *J Educ Bus*. 2014;89:202–206.
7. Youn S, Hall K. Gender and Online Privacy among Teens: Risk Perception, Privacy Concerns, and Protection Behaviors. *Cyberpsychol Behav*. 2008;11:763–765.
8. Drake J, Hall D, Becton JB, Posey C. Job Applicants' Information Privacy Protection Responses: Using Social Media for Candidate Screening. *AIS Trans Hum-Comput Interact*. 2016;8:160–184.
9. Wheeless LR. Self-Disclosure and Interpersonal Solidarity: Measurement, Validation, and Relationships. *Hum Commun Res*. 1976;3:47–61.
10. Krasnova H, Veltri NF. Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA. In: 2010 43rd Hawaii International Conference on System Sciences. ; 2010: 1–10.
11. Lutz C, Ranzini G. Where Dating Meets Data: Investigating Social and Institutional Privacy Concerns on Tinder. *Soc Media Soc*. 2017;3:2056305117697735.
12. Brady E, Segar J, Sanders C. "I Always Vet Things": Navigating Privacy and the Presentation of Self on Health Discussion Boards Among Individuals with Long-Term Conditions. *J Med Internet Res*. 2016;18:e274.
13. Burkell J, Fortier A, Wong L (Lola) YC, Simpson JL. Facebook: public space, or private space? *Inf Commun Soc*. 2014;17:974–985.
14. West A, Lewis J, Currie P. Students' Facebook 'friends': public and private spheres. *J Youth Stud*. 2009;12:615–627.
15. Lange PG. Publicly Private and Privately Public: Social Networking on YouTube. *J Comput-Mediat Commun*. 2007;13:361–380.
16. Gal S. A Semiotics of the Public/Private Distinction. *Differ J Fem Cult Stud*. 2002;13:77–95.
17. Smith HJ, Milberg SJ, Burke SJ. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Q*. 1996;20:167–196.
18. Stewart KA, Segars AH. An Empirical Examination of the Concern for Information Privacy Instrument. *Inf Syst Res*. 2002;13:36–49.

19. Li Y. A multi-level model of individual information privacy beliefs. *Electron Commer Res Appl*. 2014;13:32–44.

20. Mao E, Zhang J. Gender Differences in the Effect of Privacy on Location-Based Services Use on Mobile Phones. 2014. Available at http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1207&context=amcis2014. Accessed May 27, 2017.

21. Hew J-J, Lee V-H, Ooi K-B, Lin B. Mobile social commerce: The booster for brand loyalty? *Comput Hum Behav*. 2016;59:142–154.

22. Lowry PB, Cao J, Everard A. Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures. *J Manag Inf Syst*. 2011;27:163–200.

23. Osatuyi B. Empirical Examination of Information Privacy Concerns Instrument in the Social Media Context. *AIS Trans Replication Res*. 2015;1. Available at http://aisel.aisnet.org/trr/vol1/iss1/3.

24. Krasnova H, Günther O, Spiekermann S, Koroleva K. Privacy concerns and identity in online social networks. *Identity Inf Soc*. 2009;2:39–63.

25. Krasnova H, Veltri NF, Günther O. Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture. *Bus Inf Syst Eng*. 2012;4:127–135.

26. Lai C-Y, Yang H-L. Determinants of individuals' self-disclosure and instant information sharing behavior in micro-blogging. *New Media Soc*. 2015;17:1454–1472.

27. Kokolakis S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Comput Secur*. 2017;64:122–134.

28. Taddicken M. The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. *J Comput-Mediat Commun*. 2014;19:248–273.

29. Cheung C, Lee ZWY, Chan TKH. Self-disclosure in social networking sites: The role of perceived cost, perceived benefits and social influence. *Internet Res*. 2015;25:279–299.

30. Son J-Y, Kim SS. Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model. *MIS Q*. 2008;32:503–529.

31. Leary MR, Kowalski RM. Impression management: A literature review and two-component model. *Psychol Bull*. 1990;107:34.

32. Young AL, Quan-Haase A. Privacy Protection Strategies on Facebook. *Inf Commun Soc*. 2013;16:479–500.

33. Donath J, Boyd D. Public Displays of Connection. *BT Technol J*. 2004;22:71–82.

34. Gruzd A, Jacobson J, Dubois E. You're Hired: Examining Acceptance of Social Media Screening of Job Applicants. 2017. Available at http://aisel.aisnet.org/amcis2017/DataScience/Presentations/28/. Accessed September 29, 2017.

35. Walther JB. Interpersonal Effects in Computer-Mediated Interaction. *Commun Res*. 1992;19:52–90.

36. DeAndrea DC, Tom Tong S, Liang YJ, Levine TR, Walther JB. When Do People Misrepresent Themselves to Others? The Effects of Social Desirability, Ground Truth, and Accountability on Deceptive Self-Presentations. *J Commun*. 2012;62:400–417.

37. Bazarova NN, Taft JG, Choi YH, Cosley D. Managing Impressions and Relationships on Facebook: Self-Presentational and Relational Concerns Revealed Through the Analysis of Language Style. *J Lang Soc Psychol*. 2013;32:121–141.

38. Hallam C, Zanella G. Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Comput Hum Behav*. 2017;68:217–227.

39. Zhao L, Lu Y, Gupta S. Disclosure Intention of Location-Related Information in Location-Based Social Network Services. *Int J Electron Commer*. 2012;16:53–90.

40. Bateman PJ, Pike JC, Butler BS. To disclose or not: publicness in social networking sites. *Inf Technol People*. 2011;24:78–100.

41. Leung L. Loneliness, Self-Disclosure, and ICQ ("I Seek You") Use. *Cyberpsychol Behav*. 2002;5:241–251.

42. Cho SH. Effects of Motivations and Gender on Adolescents' Self-Disclosure in Online Chatting. *Cyberpsychol Behav*. 2007;10:339–345.

43. Christofides E, Muise A, Desmarais S. Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? *Cyberpsychol Behav*. 2009;12:341–345.

44. Hair JF, Sarstedt M, Ringle CM, Gudergan SP. Advanced issues in partial least squares structural equation modeling. Los Angeles: SAGE; 2018: 1-254.

45. Shmueli G, Ray S, Velasquez Estrada JM, Chatla SB. The elephant in the room: Predictive performance of PLS models. *J Bus Res*. 2016;69:4552–4564.

46. Henseler J, Ringle CM, Sarstedt M. Testing measurement invariance of composites using partial least squares. *Int Mark Rev*. 2016;33:405–431.

47. Henseler J, Hubona G, Ray PA. Using PLS path modeling in new technology research: updated guidelines. *Ind Manag Data Syst*. 2016;116:2–20.

48. Ringle CM, Wende S, Becker J-M. SmartPLS 3. Bönningstedt: SmartPLS. *Retrieved July*. 2015;15:2016.

49. Hair JF, Hult GTM, Ringle CM, Sarstedt M. A primer on partial least squares structural equation modeling (PLS-SEM), Second edition. Los Angeles: Sage; 2017: 1-363.

50. Alashoor T, Han S, Joseph R. Familiarity with Big Data, Privacy Concerns, and Self-disclosure Accuracy in Social Networking Websites: An APCO Model. *Commun Assoc Inf Syst*. 2017;41. Available at http://aisel.aisnet.org/cais/vol41/iss1/4.

51. Barth S, de Jong MDT. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telemat Inform*. 2017;34:1038–1058.

52. Rimé Bernard. The Social Sharing of Emotion as an Interface Between Individual and Collective Processes in the Construction of Emotional Climates. *J Soc Issues*. 2007;63:307–322.

Appendix A

Table A1: Construct Operationalization—Self-disclosure on public/private social media websites (adopted from Lai and Yang[1])

You indicated that one or more of your social media accounts is primarily PUBLIC/PRIVATE. When using your PUBLIC/PRIVATE account(s), to what extent do you agree with the following statements? (7-point agreement/disagreement scale)	
Self-disclosure amount	
SDAm1* (reversed)	I do not often talk about myself on social media
SDAm2	I usually talk about myself on social media for fairly long periods
SDAm3	I often discuss my feelings about myself on social media
SDAm4	I often express my personal beliefs and opinions on social media
Self-disclosure depth	
SDD1	I would intimately, openly, and fully disclose who I really am in my post on social media
SDD2	I typically reveal information about myself on social media without intending to
SDD3	I often disclose intimate, personal things about myself on social media without hesitation
SDD4	When I post about myself on social media, the posts are fairly detailed
Self-disclosure positive/negative matter (SDPN)	
SDPN1	I usually disclose positive things about myself on social media
SDPN2	I normally express my good feelings about myself on social media
SDPN3	On the whole, my disclosures about myself on social media are more positive than negative
Self-disclosure accuracy (SDAc)	
SDAc1	My expressions of my own feelings, emotions, and experiences on social media are true reflections of myself
SDAc2	My self-disclosures on social media are completely accurate reflections of who I really am
SDAc3	My self-disclosures on social media can accurately reflect my own feelings, emotions, and experiences
SDAc4	My statements about my own feelings, emotions, and experiences on social media are always accurate self-perceptions
Self-disclosure intention (SDI)	
SDI1	When I express my personal feelings on social media, I am always aware of what I am doing and saying
SDI2	When I reveal my feelings about myself on social media, I consciously intend to do so
SDI3	When I self-disclose on social media, I am consciously aware of what I am revealing

Table A2: Construct Operationalization—Social Threats (adopted from Krasnova et al.[2])

To what extent do you agree with the following statements (7-point agreement/disagreement scale)	
Concerns about Social Threats	
CST1	I am often concerned that someone might purposefully embarrass me on social media
CST2	It often worries me that other users might purposefully write something undesired about me on social media
CST3	I am often concerned that other users might take advantage of the information they learned about me through social media

Table A3: Construct Operationalization—Social Media Information Privacy—CFSMIP (adopted from Stewart and Segars[3], Osatuyi[4])

To what extent do you agree with the following statements (7-point agreement/disagreement scale)	
Collection (COL)	
COL1	It usually bothers me when social media sites ask me for personal information
COL2	It usually bothers me when social media sites ask me for my current location information
COL3	It bothers me to give personal information to so many people on social media
COL4	I am concerned that social media sites are collecting too much personal information about me
Errors (ERR)	
ERR1	Social media sites should take more steps to make sure that personal information in their database is accurate

ERR2	Social media sites should have better procedures to correct errors in personal information
ERR3	Social media sites should devote more time and effort to verifying the accuracy of the personal information in their databases before using it for recommendations
Secondary Use (SUS)	
SUS1	Social media sites should not use personal information for any purpose unless it has been authorized by the individuals who provide the information
SUS2	When people give personal information to social media sites for some reason, these sites should never use the information for any other purpose
SUS3	Social media sites should never share personal information with third-party entities unless authorized by the individual who provided the information
Unauthorized Access (UAC)	
UAC1	Databases that contain personal information should be protected from unauthorized access no matter how much it costs
UAC2	Social media sites should take more steps to make sure that unauthorized people cannot access personal information on their site
UAC3	Databases that contain personal information should be highly secured
UAC4	Social media sites should delete a user's account if they illegally access another user's personal information

Appendix B

Table B1: Results of internal reliability and convergent validity assessment (CFSMIP reflective-formative, Mode A)*

Internal reliability (outer loadings; for CFSMIP, outer weights)

	COL	ERR	SUS	UAC	CFS MIP	CST	SDAc		SDAD		SDPN		SDI	
							Pub.	Pri.	Pub.	Pri.	Pub.	Pri.	Pub.	Pri.
COL1	.78				.09									
COL2	.76				.09									
COL3	.80				.09									
COL4	.79				.10									
ERR1		.86			.10									
ERR2		.87			.11									
ERR3		.86			.10									
SUS1			.77		.14									
SUS2			.68		.12									
SUS3			.74		.13									
UAC1				.83	.13									
UAC2				.88	.14									
UAC3				.86	.14									
CST1						.91								
CST2						.91								
CST3						.76								
SDAc1							.87	.89						
SDAc2							.86	.89						
SDAc3							.62	.85						
SDAc4							.82	.90						
SDAm2									.89	.88				
SDAm3									.85	.84				
SDAm4									.68	.68				
SDD2									.83	.83				
SDD3									.84	.86				
SDD4									.79	.80				
SDI1													.89	.89
SDI2													.63	.85
SDI3													.84	.89
SDP1											.61	.77		
SDP3											.99	.98		

Construct reliability and convergent validity

	α		ρ_c		AVE	
	Public	Private	Public	Private	Public	Private
COL	.79		.87		.62	
ERR	.83		.90		.74	
SUS	.82		.89		.74	
UAC	.82		.89		.74	
CFSMIP	-		-		-	
CST	.83		.90		.74	
SDAc	.83	.91	.88	.93	.64	.78
SDAD	.90	.90	.92	.92	.66	.67
SDPN	.71	.76	.80	.87	.68	.78
SDI	.71	.85	.83	.91	.63	.77

* Measurement instrument after items depuration.

Note 1: Internal reliability was tested by observing composite reliability (ρ_c), with all values higher than 0.8 across both groups (well above the threshold of 0.6). Scale reliability analysis required item depuration, as some indicators were far below the cut-off level of 0.7; four items with loadings between 0.6 and 0.7 were retrieved because their deletion did not lead to significant improvement of composite reliability or average variance extracted (AVE), and to ensure content validity[5]. In total, four items were deleted, and internal reliability and scale reliability were re-tested. Convergent validity was confirmed upon observation of AVE values, which were above the threshold of 0.5[6].

Note 2: The second-order variable was measured following a reflective-formative approach, using Mode B for the higher order construct. Despite VIF values lower than 3.5, the path coefficient between collection and CFSMIP had a negative sign, which might be indicative of potential collinearity or suppression issues[7]. Therefore, following Becker et al.[8], we used Mode A for the higher order construct, calculating correlation weights instead, and re-tested the model. An additional advantage of using Mode A is that correlation weights provide superior out-of-sample prediction.

Table B2: Results of discriminant validity assessment

Heterotrait-Monotrait Ratio (HTMT)

Public

	COL	ERR	SUS	UAC	CST	SDAc	SDAD	SDPN	SDI
COL									
ERR	.55								
SUS	.63	.54							
UAC	.62	.59	.88						
CST	.59	.57	.21	.28					
SDAc	.05	.21	.16	.14	.05				
SDAD	.05	.07	.26	.24	.31	.39			
SDPN	.06	.17	.16	.16	.07	.67	.33		
SDI	.11	.22	.38	.35	.05	.67	.15	.72	

Private

	COL	ERR	SUS	UAC	CST	SDAc	SDAD	SDPN	SDI
COL									
ERR	.55								
SUS	.63	.53							
UAC	.62	.59	.88						
CST	.59	.57	.21	.28					
SDAc	.05	.20	.20	.18	.06				
SDAD	.05	.07	.22	.22	.28	.29			
SDPN	.05	.20	.23	.22	.09	.72	.22		
SDI	.12	.23	.39	.36	.05	.73	.13	.73	

Note: Based on the HTMT criterion[9], the results indicated discriminant validity issues between amount and depth of self-disclosure; considering that both concepts are related, they were grouped together (SDAD). After re-testing, all values were lower than 0.85 except for the expected higher values between second order and first order constructs, and between secondary use and unauthorized access, at 0.88, which is in line with Osatuyi's results[4] and may also explain the analysis of CFSMIP in Mode B. Both variables were kept independent to preserve content validity and because the value was lower than the less restrictive limit of 0.90.

Table B3: Results of measurement invariance assessment

	Step 2	Step 3	
	Permutation p-values	Mean (permutation p-values)	Variance (permutation p-values)
COL	-	-	-
ERR	-	-	-
SUS	-	-	-
UAC	-	-	-
CST	.90	-	-
SDAc	.35	.04	.66
SDAD	.52	.13	.45
SDPN	.58	.41	.82
SDI	.08	.79	.58

Note: Multigroup analysis requires confirming measurement invariance across groups. The choice of the same constructs and indicators ensures configural invariance. The analysis includes a MICOM test[10] with 5,000 permutations to test compositional and scalar invariance (Table B3). The results of step 2 of the MICOM test showed no significant differences across groups. However, step 3 of MICOM showed significant differences in the means of self-disclosure accuracy, and thus scalar invariance was not ensured. Given that partial measurement invariance was established, multigroup analysis is possible.

Table B4: Results of structural model assessment and multigroup analysis

	Public		Private		PLS-MGA	
	β	f^2	β	f^2	β_{diff}	p-value
COL→CFSMIP	**.29****	-	**.29****	-	.00	.52
ERR→CFSMIP	**.27****	-	**.27****	-	.00	.53
SUS→CFSMIP	**.34****	-	**.34****	-	.00	.47
UAC→CFSMIP	**.34****	-	**.34****	-	.00	.49
CFSMIP→SDAc	**.18****	.03	**.22****	.04	.04	.30
CFSMIP→SDAD	**-.30****	.09	**-.28****	.08	.02	.36
CFSMIP→SDPN	.18^{ns}	.03	**.22****	.05	.05	.33
CFSMIP→SDI	**.33****	.10	**.36****	.12	.03	.35
CST→SDAc	**-.10***	.01	**-.14****	.02	.03	.69
CST→SDAD	**.40****	.16	**.37****	.13	.03	.74
CST→SDPN	-.04^{ns}	.00	-.08^{ns}	.01	.04	.63
CST→SDI	**-.15****	.02	**-.17****	.03	.02	.63

*p<.05; **p<.01; ^{ns} non-significant

	R^2		SRMR			
	Public	Private	Saturated		Estimated	
CFSMIP	1	1	Public	Private	Public	Private
SDAc	.03	.04	.10	.10	.12	.13
SDAD	.16	.13				
SDPN	.03	.04				
SDI	.09	.11				

Note: The VIF values are below 3 in all cases (except for SDAc4, at 3.23 in the private group); therefore, the results discard potential collinearity issues. The values of R^2 are relatively low (0.03–0.16) with higher variance explained of self-disclosure amount and depth, and intent. Furthermore, the SRMR may indicate a poor fit (between 0.097 and 0.128 for the saturated and estimated models, respectively), which suggests that the model might not be sufficient to explain self-disclosure behaviors in private or public social media platforms. Finally, a blindfolding procedure with a distance omission of 7 returns positive values of Q^2, which confirms the predictive relevance of the model.

Appendix References

1. Lai C-Y, Yang H-L. Determinants of individuals' self-disclosure and instant information sharing behavior in micro-blogging. *New Media & Society*. 2015;17:1454–1472.
2. Krasnova H, Günther O, Spiekermann S, Koroleva K. Privacy concerns and identity in online social networks. *IDIS*. 2009;2:39–63.
3. Stewart KA, Segars AH. An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research*. 2002;13:36–49.
4. Osatuyi B. Empirical Examination of Information Privacy Concerns Instrument in the Social Media Context. *AIS Transactions on Replication Research*. 2015;1. Available at http://aisel.aisnet.org/trr/vol1/iss1/3.
5. Hair JF, Hult GTM, Ringle CM, Sarstedt M. A primer on partial least squares structural equation modeling (PLS-SEM), Second edition. Los Angeles: Sage; 2017: 1-363.
6. Fornell C, Larcker DF. Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*. 1981;18:39–50.
7. Rigdon EE. Rethinking Partial Least Squares Path Modeling: In Praise of Simple Methods. *Long Range Planning*. 2012;45:341–358.
8. Becker J-M, Rai A, Rigdon EE. Predictive Validity and Formative Measurement in Structural Equation Modeling: Embracing Practical Relevance. Milan: AIS Electronic Library (AISeL); 2013. Available at http://aisel.aisnet.org/icis2013/proceedings/ResearchMethods/5/.
9. Henseler J, Ringle CM, Sarstedt M. A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*. 2015;43:115–135.
10. Henseler J, Ringle CM, Sarstedt M. Testing measurement invariance of composites using partial least squares. *International Marketing Review*. 2016;33:405–431.