Cyberpsychology, Behavior, and Social Networking
Volume 21, Number 7, 2018
Mary Ann Liebert, Inc.
DOI: 10.1089/cyber.2017.0709

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

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

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 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. 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.

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

Introduction

Considering the prevalence of self-disclosure on social media, research has sought to understand what makes one 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 microtargeting in political advertisements, 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 the following:

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?

[1] Ted Rogers School of Management, Ryerson University, Toronto, Canada.
[2] Department of Organization Engineering, Business Administration and Statistics, Universidad Politécnica de Madrid, Madrid, Spain.

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 the following:

RQ3: If there is a relationship between organizational privacy and social threat 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 (CFSMIP) measurement scale.[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 (IPPRs). 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 the following:

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 the following:

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 the following:

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:

Table 1. Sample Demographics

	N	%	Avg. No. 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	545 100%		5 (2)	524 96%	431 79%	344 63%	328 60%	327 60%	280 51%	210 39%	110 20%	87 16%	96 18%

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 through 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 the following:

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.

Materials and Methods

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 545 people who had at least one public account and one private account (Table 1). The online survey was open from June 1 to July 15, 2017, and hosted by Qualtrics.

Instrument design

The measurement items used in this research have been validated by other researchers as outlined below (Appendix Tables A1–A3).

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 nonredundant tetrads are significantly different from zero.

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

The general rules for assessment follow Hair et al.[44,48] 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, and then a measurement invariance (configurational, compositional, and scalar invariance) assessment. See Appendix Tables A4–A7 for more details. Figure 1 presents the 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 are 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 (Fig. 1). H4a, however, is not supported as the path coefficient for polarity is not significant in the context of public self-disclosure.

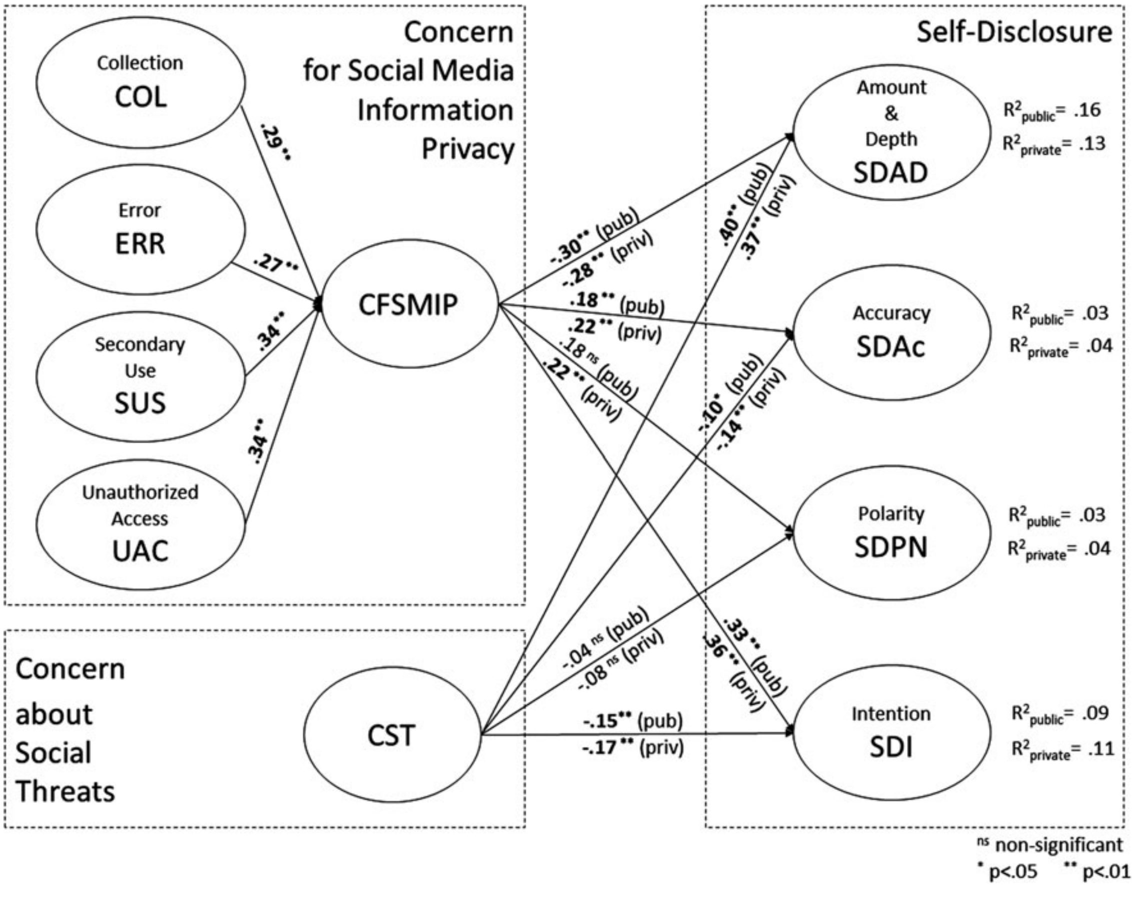

FIG. 1. Results of the structural model assessment.

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 suggest 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.[49]

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 this 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 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[27,50] 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.[37,51]

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 toward 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.

Acknowledgments

This research is supported through a five-year initiative on ''Social Media Data Stewardship'' funded by the Canada Research Chairs program (2015–2020; Principal Investigator: Gruzd, A).

Author Disclosure Statement

No competing financial interests exist.

References

1. Bauer C, Schiffinger M. (2015) Self-disclosure in online interaction: a meta-analysis. In *2015 48th Hawaii International Conference on System Sciences*. Washington, DC, IEEE Computer Society, pp. 3621–3630.
2. Wagner K. Here's how Facebook allowed Cambridge Analytica to get data for 50 million users. Recode. www.recode.net/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data (accessed Mar. 25, 2018).
3. Mack E. #DeleteFacebook trends as compromised social users fume. CNET. www.cnet.com/news/deletefacebook-hashtag-trends-twitter-facebook-users (accessed Mar. 25, 2018).
4. Culnan MJ, Armstrong PK. Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. Organization Science 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. Computers in Human Behavior 2012; 28:1859–1872.
6. Root T, McKay S. Student awareness of the use of social media screening by prospective employers. Journal of Education for Business 2014; 89:202–206.
7. Youn S, Hall K. Gender and online privacy among teens: risk perception, privacy concerns, and protection behaviors. Cyberpsychology and Behavior 2008; 11:763–765.
8. Drake J, Hall D, Becton JB, et al. Job applicants' information privacy protection responses: using social media for candidate screening. AIS Transactions on Human-Computer Interaction 2016; 8:160–184.
9. Wheeless LR. Self-disclosure and interpersonal solidarity: measurement, validation, and relationships. Human Communication Research 1976; 3:47–61.
10. Krasnova H, Veltri NF. (2010) Privacy calculus on social networking sites: explorative evidence from Germany and USA. In: *2010 43rd Hawaii International Conference on System Sciences*. pp. 1–10.
11. Lutz C, Ranzini G. Where dating meets data: investigating social and institutional privacy concerns on tinder. Social Media and Society 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. Journal of Medical Internet Research 2016; 18:e274.
13. Burkell J, Fortier A, Wong L (Lola) YC, et al. Facebook: public space, or private space? Information, Communication and Society 2014; 17:974–985.
14. West A, Lewis J, Currie P. Students' Facebook 'friends': public and private spheres. Journal of Youth Studies 2009; 12:615–627.
15. Lange PG. Publicly private and privately public: social networking on YouTube. Journal of Comput-Mediated Communication 2007; 13:361–380.
16. Gal S. A semiotics of the public/private distinction. Differences: A Journal of Feminist Cultural Studies 2002; 13:77–95.
17. Smith HJ, Milberg SJ, Burke SJ. Information privacy: measuring individuals' concerns about organizational practices. MIS Quarterly 1996; 20:167–196.
18. Stewart KA, Segars AH. An empirical examination of the concern for information privacy instrument. Information System Research 2002; 13:36–49.
19. Li Y. A multi-level model of individual information privacy beliefs. Electronic Commerce Research and Applications 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. 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, et al. Mobile social commerce: the booster for brand loyalty? Computers in Human Behavior 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. Journal of Management Information Systems 2011; 27:163–200.
23. Osatuyi B. Empirical examination of information privacy concerns instrument in the social media context. AIS Transactions on Replication Research 2015; 1: 1–14.
24. Krasnova H, Günther O, Spiekermann S, et al. Privacy concerns and identity in online social networks. Identity in the Information Society 2009; 2:39–63.
25. Krasnova H, Veltri NF, Günther O. Self-disclosure and privacy calculus on social networking sites: the role of culture. Business and Information Systems Engineering 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 and Society 2015; 17:1454–1472.
27. Kokolakis S. Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. Computers and Security 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. Journal of Computer-Mediated Communication 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 Research 2015; 25:279–299.
30. Son J-Y, Kim SS. Internet users' information privacy-protective responses: a taxonomy and a nomological model. MIS Quarterly 2008; 32:503–529.
31. Leary MR, Kowalski RM. Impression management: a literature review and two-component model. Psychological Bulletin 1990; 107:34.
32. Young AL, Quan-Haase A. Privacy protection strategies on Facebook. Information, Communication and Society 2013; 16:479–500.
33. Donath J, Boyd D. Public displays of connection. BT Technology Journal 2004; 22:71–82.

34. Gruzd A, Jacobson J, Dubois E. You're hired: examining acceptance of social media screening of job applicants. 2017. http://aisel.aisnet.org/amcis2017/DataScience/Presentations/28 (accessed Sep. 29, 2017).
35. Walther JB. Interpersonal effects in computer-mediated interaction. Communication Research 1992; 19:52–90.
36. DeAndrea DC, Tom Tong S, Liang YJ, et al. When do people misrepresent themselves to others? The effects of social desirability, ground truth, and accountability on deceptive self-presentations. Journal of Communication 2012; 62:400–417.
37. Bazarova NN, Taft JG, Choi YH, et al. Managing impressions and relationships on Facebook: self-presentational and relational concerns revealed through the analysis of language style. Journal of Language and Social Psychology 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. Computers in Human Behavior 2017; 68:217–227.
39. Zhao L, Lu Y, Gupta S. Disclosure intention of location-related information in location-based social network services. International Journal of Electronic Commerce 2012; 16:53–90.
40. Bateman PJ, Pike JC, Butler BS. To disclose or not: publicness in social networking sites. Information Technology and People 2011; 24:78–100.
41. Leung L. Loneliness, self-disclosure, and ICQ ("i seek you") use. Cyberpsychology and Behavior 2002; 5:241–251.
42. Cho SH. Effects of motivations and gender on adolescents' self-disclosure in online chatting. Cyberpsychology and Behaviour 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? Cyberpsychology and Behaviour 2009; 12:341–345.
44. Hair JF, Sarstedt M, Ringle CM, et al. (2018). *Advanced issues in partial least squares structural equation modeling.* Los Angeles: SAGE, pp. 1–254.
45. Shmueli G, Ray S, Velasquez Estrada JM, et al. The elephant in the room: predictive performance of PLS models. Journal of Business Research 2016; 69:4552–4564.
46. Henseler J, Ringle CM, Sarstedt M. Testing measurement invariance of composites using partial least squares. International Marketing Review 2016; 33:405–431.
47. Henseler J, Hubona G, Ray PA. Using PLS path modeling in new technology research: updated guidelines. Industrial Management and Data Systems 2016; 116:2–20.
48. Hair JF, Hult GTM, Ringle CM, et al. *A primer on partial least squares structural equation modeling (PLS-SEM).* 2nd ed. Los Angeles: Sage; 2017: 1–363.
49. Alashoor T, Han S, Joseph R. Familiarity with big data, privacy concerns, and self-disclosure accuracy in social networking websites: an APCO model. Communications of Association for Information Systems 2017; 41. http://aisel.aisnet.org/cais/vol41/iss1/4.
50. Barth S, de Jong MDT. The privacy paradox—investigating discrepancies between expressed privacy concerns and actual online behavior—a systematic literature review. Telematics and Informatics 2017; 34:1038–1058.
51. Rimé B. The social sharing of emotion as an interface between individual and collective processes in the construction of emotional climates. Journal of Social Issues 2007; 63:307–322.

Address correspondence to:
Dr. Anatoliy Gruzd
Ted Rogers School of Management
Ryerson University
350 Victoria Street
Toronto M5B 2K3
Ontario
Canada

E-mail: gruzd@ryerson.ca

Appendix

Appendix Table A1. Construct Operationalization: Self-Disclosure on Public/Private Social Media Web Sites

You indicated that one or more of your social media accounts are 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	
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

(*continued*)

Appendix Table A1. (Continued)

You indicated that one or more of your social media accounts are 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 accuracy	
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	
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

Adopted from Lai and Yang.[A1]

*The scale for this question is reversed.

SDAm, self-disclosure amount; SDD, self-disclosure depth; SDPN, self-disclosure positive/negative matter; SDAc, self-disclosure accuracy; SDI, self-disclosure intention.

Appendix Table A2. Construct Operationalization: Concern About Social Threats

To what extent do you agree with the following statements (7-point agreement/disagreement scale)

Concern 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

Adopted from Krasnova et al.[A2]

CST, Concern about Social Threats.

Appendix Table A3. Construct Operationalization—Concern for Social Media Information Privacy—CFSMIP

To what extent do you agree with the following statements (7-point agreement/disagreement scale)

Collection	
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	
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	
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	
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

Adopted from Stewart and Segars[A3] and Osatuyi.[A4]

CFSMIP, Concern for Social Media Information Privacy; COL, collection; ERR, errors; SUS, secondary use; UAC, unauthorized access.

Appendix Table A4. Results of Internal Reliability and Convergent Validity Assessment (CFSMIP Reflective-Formative, Mode A)

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

							SDAc		*SDAD*		*SDPN*		*SDI*	
	COL	*ERR*	*SUS*	*UAC*	*CFSMIP*	*CST*	*Pub.*	*Pri.*	*Pub.*	*Pri.*	*Pub.*	*Pri.*	*Pub.*	*Pri.*
COL1	0.78				0.09									
COL2	0.76				0.09									
COL3	0.80				0.09									
COL4	0.79				0.10									
ERR1		0.86			0.10									
ERR2		0.87			0.11									
ERR3		0.86			0.10									
SUS1			0.77		0.14									
SUS2			0.68		0.12									
SUS3			0.74		0.13									
UAC1				0.83	0.13									
UAC2				0.88	0.14									
UAC3				0.86	0.14									
CST1						0.91								
CST2						0.91								
CST3						0.76								
SDAc1							0.87	0.89						
SDAc2							0.86	0.89						
SDAc3							0.62	0.85						
SDAc4							0.82	0.90						
SDAm2									0.89	0.88				
SDAm3									0.85	0.84				
SDAm4									0.68	0.68				
SDD2									0.83	0.83				
SDD3									0.84	0.86				
SDD4									0.79	0.80				
SDI1													0.89	0.89
SDI2													0.63	0.85
SDI3													0.84	0.89
SDP1											0.61	0.77		
SDP3											0.99	0.98		

Construct reliability and convergent validity

	α		ρ_c		*AVE*	
	Public	*Private*	*Public*	*Private*	*Public*	*Private*
COL	0.79		0.87		0.62	
ERR	0.83		0.90		0.74	
SUS	0.82		0.89		0.74	
UAC	0.82		0.89		0.74	
CFSMIP	—		—		—	
CST	0.83		0.90		0.74	
SDAc	0.83	0.91	0.88	0.93	0.64	0.78
SDAD	0.90	0.90	0.92	0.92	0.66	0.67
SDPN	0.71	0.76	0.80	0.87	0.68	0.78
SDI	0.71	0.85	0.83	0.91	0.63	0.77

Measurement instrument after item 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 cutoff 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 AVE, and to ensure content validity.[A5] In total, four items were deleted, and internal reliability and scale reliability were retested. Convergent validity was confirmed upon observation of AVE values, which were above the threshold of 0.5.[A6] 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.[A7] Therefore, following Becker et al.,[A8] we used Mode A for the higher order construct, calculating correlation weights instead, and retested the model. An additional advantage of using Mode A is that correlation weights provide superior out-of-sample prediction.

AVE, average variance extracted; VIF, variance inflation factor.

Appendix Table A5. Results of Discriminant Validity Assessment

Heterotrait-Monotrait ratio

	COL	*ERR*	*SUS*	*UAC*	*CST*	*SDAc*	*SDAD*	*SDPN*	*SDI*
Public									
COL									
ERR	0.55								
SUS	0.63	0.54							
UAC	0.62	0.59	0.88						
CST	0.59	0.57	0.21	0.28					
SDAc	0.05	0.21	0.16	0.14	0.05				
SDAD	0.05	0.07	0.26	0.24	0.31	0.39			
SDPN	0.06	0.17	0.16	0.16	0.07	0.67	0.33		
SDI	0.11	0.22	0.38	0.35	0.05	0.67	0.15	0.72	
Private									
COL									
ERR	0.55								
SUS	0.63	0.53							
UAC	0.62	0.59	0.88						
CST	0.59	0.57	0.21	0.28					
SDAc	0.05	0.20	0.20	0.18	0.06				
SDAD	0.05	0.07	0.22	0.22	0.28	0.29			
SDPN	0.05	0.20	0.23	0.22	0.09	0.72	0.22		
SDI	0.12	0.23	0.39	0.36	0.05	0.73	0.13	0.73	

Note: Based on the HTMT criterion,[A9] 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 retesting, 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,[A4] 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.

HTMT, Heterotrait-Monotrait ratio of correlations.

Appendix Table A6. 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	0.90	—	—
SDAc	0.35	0.04	0.66
SDAD	0.52	0.13	0.45
SDPN	0.58	0.41	0.82
SDI	0.08	0.79	0.58

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[A10] with 5,000 permutations to test compositional and scalar invariance (Table A6). The results of step 2 of the MICOM test showed no significant difference 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.

MICOM, measurement invariance of composite models.

Appendix Table A7. Results of Structural Model Assessment and Multigroup Analysis

	Public		*Private*		*PLS-MGA*	
	β	f^2	*β*	f^2	β_{diff}	p
COL → CFSMIP	0.29**	—	0.29**	—	0.00	0.52
ERR → CFSMIP	0.27**	—	0.27**	—	0.00	0.53
SUS → CFSMIP	0.34**	—	0.34**	—	0.00	0.47
UAC → CFSMIP	0.34**	—	0.34**	—	0.00	0.49
CFSMIP → SDAc	0.18**	0.03	0.22**	0.04	0.04	0.30
CFSMIP → SDAD	−0.30**	0.09	−0.28**	0.08	0.02	0.36
CFSMIP → SDPN	0.18[a]	0.03	0.22**	0.05	0.05	0.33
CFSMIP → SDI	0.33**	0.10	0.36**	0.12	0.03	0.35
CST → SDAc	−0.10*	0.01	−0.14**	0.02	0.03	0.69
CST → SDAD	0.40**	0.16	0.37**	0.13	0.03	0.74
CST → SDPN	–0.04[a]	0.00	–0.08[a]	0.01	0.04	0.63
CST → SDI	−0.15**	0.02	−0.17**	0.03	0.02	0.63

	R^2		*SRMR*			
	Public	*Private*	*Saturated*		*Estimated*	
CFSMIP	1	1	Public	Private	Public	Private
SDAc	0.03	0.04	0.10	0.10	0.12	0.13
SDAD	0.16	0.13				
SDPN	0.03	0.04				
SDI	0.09	0.11				

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.

[a] ns, nonsignificant.

$*p < 0.05$; $**p < 0.01$.

PLS-MGA, partial least squares multigroup analysis.

Appendix References

A1. Lai C-Y, Yang H-L. Determinants of individuals' self-disclosure and instant information sharing behavior in micro-blogging. New Media and Society 2015; 17:1454–1472.

A2. Krasnova H, Günther O, Spiekermann S, et al. Privacy concerns and identity in online social networks. Identity in the Information Society 2009; 2:39–63.

A3. Stewart KA, Segars AH. An empirical examination of the concern for information privacy instrument. Information Systems Research 2002; 13:36–49.

A4. Osatuyi B. Empirical examination of information privacy concerns instrument in the social media context. AIS Transactions on Replication Researach 2015; 1: 1–14.

A5. Hair JF, Hult GTM, Ringle CM, et al. (2017) *A primer on partial least squares structural equation modeling (PLS-SEM).* 2nd ed. Los Angeles, pp. 1–363.

A6. Fornell C, Larcker DF. Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research 1981; 18:39–50.

A7. Rigdon EE. Rethinking partial least squares path modeling: in praise of simple methods. Long Range Planning 2012; 45:341–358.

A8. Becker J-M, Rai A, Rigdon EE. (2013) *Predictive validity and formative measurement in structural equation modeling: embracing practical relevance*. Milan: AIS Electronic Library (AISeL).

A9. Henseler J, Ringle CM, Sarstedt M. A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of Academy of Marketing Science 2015; 43:115–135.

A10. Henseler J, Ringle CM, Sarstedt M. Testing measurement invariance of composites using partial least squares. International Marketing Review 2016; 33:405–431.