Supplementary Online Appendices

Enhancing User Privacy Through Ephemeral Sharing Design:
Experimental Evidence from Online Dating

Appendix A. Social Privacy Concerns

Our survey on the literature on privacy in online dating as well as the user interviews suggested that privacy concerns primarily originate from the social interactions on the platform, which can be conceptualized as social privacy concerns. Therefore, we theorized that social privacy concerns should exhibit four dimensions—privacy concerns regarding data collection, data dissemination, identity disclosure, and identity abuse (See Table A1). One facet of social privacy concerns is the user's perceived risks associated with the disclosure of personal information, such that the information would be purposively saved or disseminated. In parallel, users' concerns regarding their social identity are prominent, as matchmaking with strangers escalates a host of privacy risks associated with users' identities. Note that in social media platforms where users connect with their offline friends or friends of friends, they do not bear the pressure of being identified by offline friends, families, or co-workers. However, in online dating platforms where bridging with potential dating partners is the ultimate goal, it is embarrassing to be re-identified by users who are normally offline friends or acquaintances (Cobb and Kohno 2017). Moreover, users of online dating platforms are more sensitive to identity-related misuse behaviors. For example, as a user's profile is exposed to strangers, the user will likely perceive that the personal information is at greater risk of being misused, such as identity theft, catfishing, and dating scams (Lutz and Ranzini 2017).

Table A1. Conceptualization of Social Privacy Concerns in Online Dating

Dimension	***Definition***	***Examples of Privacy Risks***
Data Collection Concerns	Concerns or negative feelings that other users will **collect** the shared personal information	Other users purposively save focal users' photos on their device
Data Dissemination Concerns	Concerns or negative feelings that other users will **disseminate** the shared personal information	Other users publish personal information without the focal user's consent Nonconsensual sharing of explicit content
Identity Disclosure Concerns	Concerns or negative feelings that the focal user's real **identity** can be **recognized** by other users from the shared personal information	Uncomfortable feelings (e.g., embarrassment) when identified by offline friends, co-workers, or acquaintances Concerns about getting connected with social accounts
Identity Abuse Concerns	Concerns or negative feelings that the other users will **abuse the identity** for illegal use from the shared personal information	Cyberstalking, harassment, and identity theft Using the shared photo in dating scams and catfishing

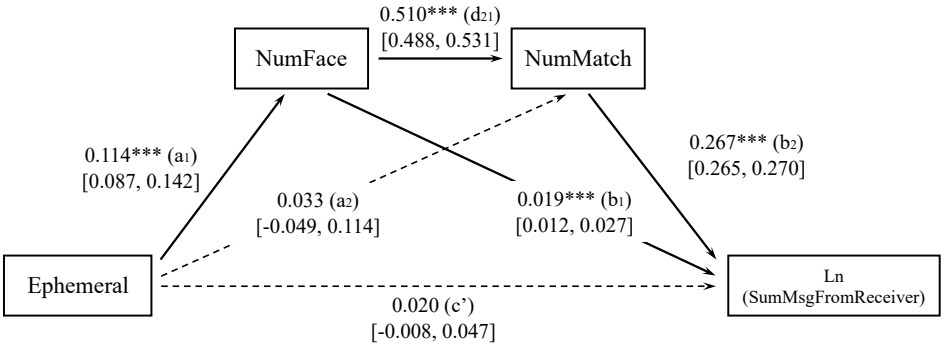
References

Cobb C, Kohno T (2017) How public is my private life? Privacy in online dating. *Proceedings of the 26th International Conference on World Wide Web (WWW)* (Perth, Australia), 1231–1240.

Lutz C, Ranzini G (2017) Where dating meets data: Investigating social and institutional privacy concerns on Tinder. *Social Media+ Society* 3(1):1–12.

Appendix B. Mediation Analysis

Figure B1. Sequential Mediation Analysis Using *NumFace* and *NumMatch* as Mediators



Note: The estimated indirect effects (Hayes 2017): **$a_1 \rightarrow d_{21} \rightarrow b_2$: 0.0155** [95% CI: 0.0112, 0.0203]; **$a_1 \rightarrow b_1$: 0.0022** [95% CI: 0.0007, 0.0040]; $a_2 \rightarrow b_2$: 0.0087 [95% CI: -0.0133, 0.0305].

Appendix C. Feature Extraction

Here, we elaborate on the process of how we extracted facial features. For each photo, we first used OpenCV to pad and resize the photo to 1024 × 1024, thereby ensuring that the size of the photo does not exceed the limit on Baidu face detection API. We then took advantage of Baidu API to determine whether each photo includes a human face and, simultaneously, to retrieve a series of facial attributes when the photo does include a human face. Then, we aggregate the interpretable attributes to the user (sender) level, as explained in Table 8 in the main text.

Further, we proxied disturbing content with *Explicit* and *Nude*, two variables extracted using image recognition methods. We applied a disturbing content detection model that classifies each photo into one of five categories, including "drawing," "hentai," "neutral," "porn," and "sexy." The model achieves an accuracy of 93% and is the most highly-rated classifier of disturbing content. If a photo is classified as "porn," "hentai," or "sexy," we deemed it as an explicit photo. Similarly, if a photo is categorized as "porn" or "hentai," we deemed it a nude photo. We use two measures for cross-validation.

Appendix D. Facial Attractiveness Prediction Process

To predict facial attractiveness, we collected a unique crowdsourced data set. Figure D1 illustrates the *Beauty Rating*, a crowdsourcing beauty rating board on the platform. In *Beauty Rating*, users can share a photo of themselves that includes their facial appearance, and any other user can rate their facial attractiveness. We used the rating data in *Beauty Rating* (*versus the open-source data set*) for two reasons. First, the photos posted on *Beauty Rating* are similar to the photos uploaded in the matching request, both of which are personal in daily life but not standardized in the open-source data set. Second, since the photos in *Beauty Rating* are rated by users on the platform, the rating better reflects their aesthetics. As the users who rate on *Beauty Rating* and those who receive the matching requests come from a homogenous group, the esthetics learned from *Beauty Rating* can be applied to receivers' preferences regarding the sender's physical appearance. Accordingly, the features extracted from *Beauty Rating* are more applicable when the model processes the photos attached to the matching requests.

The data set includes the posts and ratings from June 20, 2019, to October 16, 2019, from the transactional database.[1] It must be noted that the users can attach more than one photo to each post and the ratings of those posts reflect an overall impression on a group of photos. To make a bijection between labels and photos, we only retained the posts that only encompass one photo (hereafter, we use photo and post interchangeably). Moreover, we excluded the photos with less than 30 ratings to reduce random error (Gray et al. 2010). Further, we used the mean value of all the ratings on this photo as the label for each photo.

Figure D1. Screenshot of *Beauty Rating*

We built and trained our prediction model following the TransFBP method, the best method in both the ECCV HotOrNot competition and the SCUT-FBP competition in 2018 (Xu et al. 2018).[2] Before extracting features, we padded and resized each photo to 1024 × 1024 and fed the standardized photo to Baidu face detection API (hereafter Baidu API) to identify and locate the human face. When a human face is detected in a focal photo, we used OpenCV to separate the facial region based on the landmarks extracted by Baidu API and then padded and resized this region to a 224 × 224 photo. We then leveraged

[1] On October 16, 2019, the platform launched a new feature in Beauty Rating, which might have affected the ratings of facial attractiveness; thus, we only keep the data before the release day.

[2] Open-source code can be found at https://github.com/lucasxlu/TransFBP.

Alibaba Cloud API to extract 1024 deep features for each photo.[3] We used Alibaba Cloud API rather than other pre-trained deep learning models, such as VGG used by Xu et al. (2018). The number of features obtained by Alibaba Cloud API is substantially less than those obtained from pre-trained deep learning models, with millions of features, so our model could lower the risk of over-fitting and reduce computation complexity. We then fed the features into the Bayesian Ridge Regressor and took the facial attractiveness as the output. Finally, we randomly distributed the 1141 photos that successfully passed all the preprocesses into the training set and test set (8:2), which were leveraged to train and evaluate our model, respectively. Table D1 reports the performance of our model in terms of mean absolute error (MAE), root mean square error (RMSE), and Pearson correlation coefficient (PC).[4]

We then compared the performance with TransFBP, as the label scales from 1 to 10 in both models. Furthermore, we benchmarked TransFBP's performance on ECCV HotOrNot as HotOrNot is an online dating platform, with a similar dating context. The result revealed that our model outperformed the benchmark model on the three metrics (MAE = 1.1343, RMSE = 0.9036, and PC = 0.4676). In addition, we compared our model with the beauty prediction models in two pieces of empirical works: i) Malik et al. (2019) used a seven-scale label, and their reported RMSE on real-world data was 0.92; ii) Shi et al. (2020) used a five-scale label and their reported MAE on SCUP-FBP dataset, a standardized ID photo dataset, was 0.24. The comparisons indicated that our proposed model is among the state-of-the-art models. Then, we applied the model to predict the facial attractiveness of faces disclosed in the photos attached to the matching request and used the prediction results in empirical analysis.

Table D1. Model Performance

	MAE	***RMSE***	***PC***
1	0.5739	0.7407	0.6578
2	0.5343	0.7292	0.6999
3	0.5923	0.7617	0.6982
4	0.5785	0.7461	0.7039
5	0.5852	0.7424	0.6479
Average	0.5728	0.7440	0.6815

References

Gray D, Yu K, Xu W, Gong Y(2010) Predicting facial beauty without landmarks. In *European Conference on Computer Vision* (Springer, Berlin, Heidelberg), 434–447.

Malik N, Singh P V, Srinivasan K (2023). When does beauty pay? A large-scale image-based appearance analysis on career transitions. *Information Systems Research forthcoming*.

Shi L, Viswanathan S (2022) Optional verification and signaling in online matching markets: Evidence from a randomized field experiment. *Information Systems Research forthcoming*.

Xu L, Xiang J, Yuan X (2018) Transferring rich deep features for facial beauty prediction. *arXiv preprint arXiv:1803.07253*.

[3] Some of the faces are not sufficiently clear for deep feature extraction because of blurriness, completeness, and other potential reasons. The process is automated by Alibaba Cloud API: https://help.aliyun.com/document_detail/151968.html?spm=a2c4g.11186623.2.20.55b24c687yefdY#doc-api-facebody-RecognizeFace.

[4] For MAE and RMSE, the smaller, the better. For PC, the larger, the better. It is worth noting that the metrics will also be affected by the scale of the label.

Appendix E. Online Survey-based Experiment

We conducted an online experiment to test whether the reduced social privacy concerns are the mechanism for the effect of ephemeral sharing on users' voluntary disclosure of personal photos. Note that we also leveraged the online experiment to rule out the alternative explanations: institutional privacy concerns and self-presentation intention.

Participant. The online experiment invited participants online through *Sojump*, a popular survey and experiment platform in China, identical to *Qualtrics* (Lien et al. 2017). One hundred and five participants completed the experiment. The participants were either students whose educational backgrounds are similar to the users of our partner platform or professionals with experience in product design in leading digital platforms. We believe both groups of users can provide reliable and knowledgeable responses. Before the experiment, we determined the sample size following the well-recognized "10-times rule" approach that the number of observations should at least reach ten times the maximum number of inner or outside paths for any latent variable, and in our study 9 paths for self-disclosure intention (Goodhue et al. 2012).

Procedure. We deployed a between-subjects design in which participants were randomly assigned to either the treatment condition (hereafter referred to as the ephemeral condition, N = 53) or the persistent photo condition (hereafter referred to as the persistent condition, N = 52). Here, we briefly introduce the procedure. When first landing on the survey, a participant read a cover story that the participant was invited to experience a newly launched photo feature on our partner platform. Moreover, we briefly described our partner platform to help the participants familiarize themselves with the research context. The participants were instructed to put themselves in a scenario wherein they were to send a matching request to a prospective date.

Then, each participant was randomly assigned to either the ephemeral or persistent condition. In either group, the participants were mandated to watch a video clip regarding the photo feature in the matching process. The experiment required the participants to remain on the video page for at least 35 seconds, which was 5 seconds longer than the duration of the video clip. The video clip visualized either the ephemeral or persistent photo feature in the matching process, depending on the assigned group. Since all participants were Chinese, we delivered the video in Mandarin Chinese.

Then, the participants completed a questionnaire on attention checks, manipulation checks, main constructs, and demographics. First, the participants were mandated to answer two attention-check questions. One question pertained to the nature of the platform in the video (online dating platform, professional platform, social media platform, or other platforms) and the other question let the participants select the media of the material that the request would be sent in (photo, video, text, or other format). Then, the participants selected their perceptions regarding the main constructs, including self-disclosure intention, social privacy concerns, and constructs of alternative mechanisms, respectively. Last, the participants self-identified their age, gender, and profession. A participant, after the experiment, received a randomly drawn amount reward (in Chinese Yuan) ranging from $1 to $2, a fair payment rate in China for a survey.

Stimulus. We used a video clip as a stimulus, as the video could engage participants and easily process the information. To minimize potential confounding factors, we controlled as many factors as possible, including the visual, vocal, and script characteristics between the videos in the treatment and control groups. First, the two videos were made with the same time duration (30 seconds), the same pace in almost every clip, the same voice, the same visual stimulus (except for the burning fire and messages from our randomized field experiment), and—more importantly—the same script, except the words about the nature of the photo feature. A group of seven users of online dating platforms and five internal researchers reviewed the video clips, respectively. Accordingly, we iterated the video stimuli five times to eliminate potential ambiguity in delivering our manipulation.

Note that, most of the visual stimuli in the video originated from screenshots of the photo features in the randomized field experiment to ensure that the subjects in the online experiment underwent a similar psychological process to that in the field experiment. More importantly, the scripts in the two

scenarios were almost the same, except for the words describing the nature of the photo (ephemeral or persistent). Specifically, in the treatment condition, we highlighted the ephemeral nature of the photo (see the words in bold in *Ephemeral condition*), while we made the participants aware of the persistent nature of the photo in the persistent condition (see the words in bold in *Persistent condition*). Note that we refrained from words such as "persistent" or "permanent," since these words in Chinese can significantly draw a user's attention to potential privacy risks, which will lead to a potential overestimation of the effect of ephemeral sharing on mitigating privacy concerns.

Ephemeral condition: *Welcome to learning about the* ***ephemeral*** *photo of XXX [name of our partner platform], an online dating platform.* ***An ephemeral*** *photo is the photo feature you can leverage when sending a matching request to other users. If you are interested in a user and wish to connect with her/him, you can voluntarily include an* ***ephemeral*** *photo in your matching request, which will represent you.*
Note that when the other user receives your request, she/he can screen your request, particularly your personal photo. ***After being viewed for five seconds, the photo will be automatically burnt away and can no longer be accessed by the receiver****. Moreover,* ***the receiver cannot take a screenshot of the personal photo****. A sincere photo can leave a good first impression. Join us and send your first* ***ephemeral*** *photo!*

Persistent condition: *Welcome to learning about the* ***personal*** *photo of XXX [name of our partner platform], an online dating platform.* ***A personal*** *photo is a photo feature that you can leverage when sending a matching request to other users. If you are interested in a user and wish to connect with her/him, you can voluntarily upload a* ***personal*** *photo into your matching request, which will represent you.*
Note that when the other user receives your request, she/he can screen your request, particularly your personal photo. ***After being viewed by the receiver, the photo will remain in the matching request and can be accessed again****.* ***Specifically****,* ***the receiver can revisit the request and review the personal photo****. A sincere photo can leave a good first impression. Join us and send your first* ***personal*** *photo!*

Descriptive Statistics and Checks. From among 105 participants, 99 passed both attention checks, and we excluded the participants who failed in either check (N = 6). The ready-for-analysis sample included 50 participants in the ephemeral condition and 49 in the persistent condition. Table E1 summarizes the demographics of the participants.

Table E1. Participant Demographics

Age		***Gender***		***Profession***	
Choice	Freq.	Choice	Freq.	Choice	Freq.
19-25	76	Female	37	Student, not searching for a job	62
26-30	10	Male	62	A student searching for a job	10
31-40	11			At work	24
Above 40	2			Other	3

Note: The unit of variable age is a year.

Our tests on the demographics revealed that randomization was successfully implemented. Specifically, our *t*-test on gender did not report any significant variations in the gender composition ($p = 0.488$). The Kolmogorov–Smirnov tests on age and profession, respectively, revealed no systematic differences in the distribution of age ($p = 0.976$) and profession ($p = 0.767$).
Instrument and Validation. Due to the limit of space, we have outlined the constructs and their corresponding measures in Table E6. Note that we developed measures for social privacy concerns due to a lack of an established measure. For other measures, particularly self-disclosure intention, institutional privacy concerns, and self-presentation intention, we adapted the measures from the literature on privacy

in peer-related contexts. We adopted the most frequently used seven-point Likert scale (where 1 is "strongly disagree" and 7 is "strongly agree").[5]

We assessed the measurement model using partial least squares regression, taking a similar procedure to Jiang et al. (2013). Specifically, all the Cronbach's alpha values in Table E2 exceed 0.800, thereby indicating that the constructs exhibit adequate internal consistency (Hair et al. 2022). Besides, the composite reliability passes the threshold of 0.707, an alternative indicator of appropriate internal consistency (Hair et al. 2022). The convergent validity is justified as the average variance extracted (AVE) for all constructs and is greater than 0.500 (Fornell and Larcker, 1981).

Table E2. Construct Reliability and Validity

Variables	***Mean***	***Standard Deviation***	***Cronbach's Alpha***	***Composite Reliability***	***AVE***
Self-disclosure Intention	2.929	1.770	0.819	0.917	0.847
Data Collection Concerns	5.530	1.322	0.866	0.937	0.882
Data Dissemination Concerns	5.667	1.344	0.972	0.986	0.973
Identity Disclosure Concerns	5.869	1.167	0.820	0.917	0.848
Identity Abuse Concerns	5.606	1.443	0.924	0.963	0.929
Institutional Privacy Concerns	5.884	1.156	0.907	0.956	0.915
Self-presentation Intention	5.035	1.429	0.826	0.913	0.840

Tables E3 and E4 cross-validate the discriminant validity of constructs. First, Table E3 reports the heterotrait-monotrait (HTMT) ratio of correlations. Specifically, the HTMT values of all constructs are smaller than the HTMT criterion (0.850), the most updated criterion, which is superior to the Fornell-Larcker criterion and (partial) cross-loadings (Henseler et al. 2015). Second, as a robustness check of the results in Tables E3, Table E4 showcases that the constructs meet the Fornell and Larcker criterion in that the square root of AVE for each variable is greater than the absolute value of the correlations with other variables (Fornell and Larcker1981). The assessments together suggest adequate discriminant validity of constructs.

Table E3. Assessment of Discriminant Validity—HTMT

NO.	***Variables***	***V1***	***V2***	***V3***	***V4***	***V5***	***V6***	***V7***
V1	Self-disclosure Intention							
V2	Data Collection Concerns	0.735						
V3	Data Dissemination Concerns	0.826	0.730					
V4	Identity Disclosure Concerns	0.542	0.603	0.652				
V5	Identity Abuse Concerns	0.776	0.596	0.713	0.447			
V6	Institutional Privacy Concerns	0.603	0.382	0.475	0.619	0.660		
V7	Self-presentation Intention	0.270	0.137	0.085	0.082	0.065	0.050	

Note: The off-diagonal values are HTMT values.

Table E4. Assessment of Discriminant Validity—Fornell & Larcker Criterion

NO.	***Variables***	***V1***	***V2***	***V3***	***V4***	***V5***	***V6***	***V7***
V1	Self-disclosure Intention	0.920						
V2	Data Collection Concerns	-0.620	0.939					

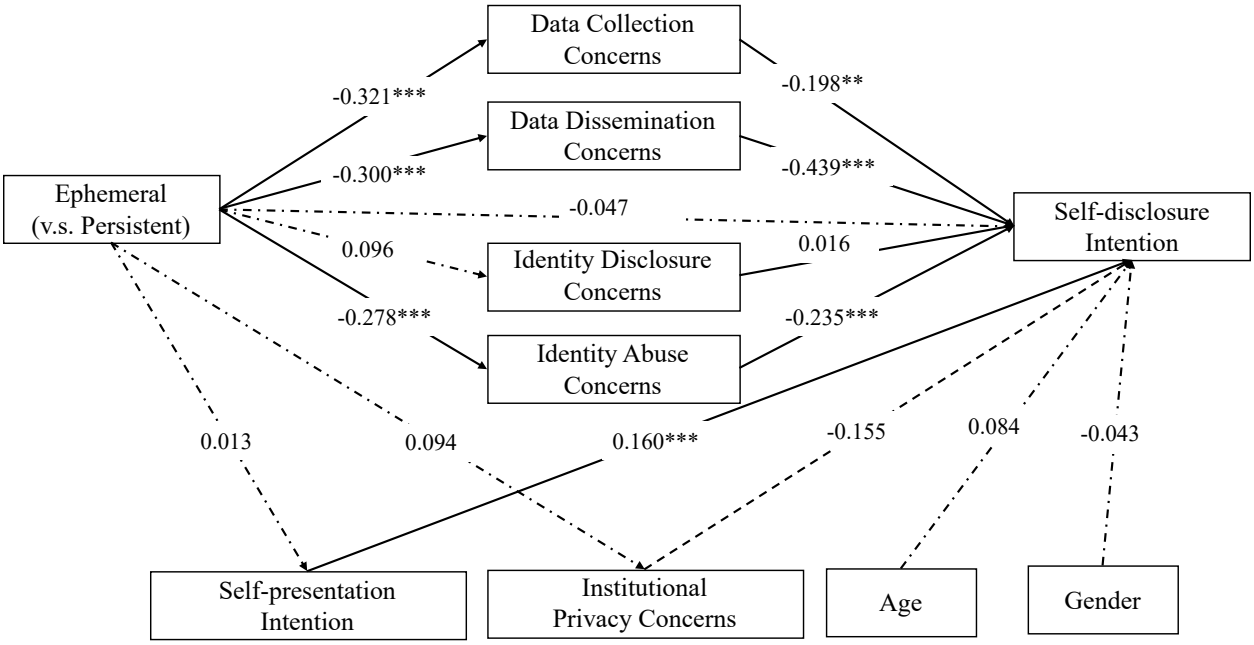
[5] We first validated all the instruments in a pretest. The table for the main constructs, definitions, and measurements will be available upon request.

V3	Data Dissemination Concerns	-0.738	0.671	0.986				
V4	Identity Disclosure Concerns	-0.445	0.509	0.583	0.921			
V5	Identity Abuse Concerns	-0.676	0.536	0.676	0.389	0.964		
V6	Institutional Privacy Concerns	-0.520	0.339	0.447	0.532	0.606	0.957	
V7	Self-presentation Intention	0.240	-0.123	-0.089	0.031	-0.010	-0.021	0.916

Note: The off-diagonal values are correlations between variables, and the diagonal values are the square roots of AVEs.

Main Results. We deployed partial least squares structural equation modeling (PSL-SEM) to test the mechanisms, as this method excels at testing complex structural models with numerous latent constructs (Hair et al. 2022; Jiang et al. 2013).[6] We used a bootstrapping algorithm with 1000 iterations to generate the path coefficients. Our PLS-SEM model in Figure E1 generates three key findings.

Figure E1. PLS-SEM Model Analyses



Note: $p < 0.1$, $p < 0.05$ **, $p < 0.01$ ****

First, the model indicates that ephemeral sharing significantly mitigates the data collection and dissemination concerns. Specifically, the path from ephemeral to data collection concerns is negative and significant ($\beta_{Ephemeral \rightarrow Data\ Collection\ Concerns}$= -0.321, $p < 0.01$), as is the path from ephemeral to data dissemination concerns ($\beta_{Ephemeral \rightarrow Data\ Dissemination\ Concerns}$= -0.300, $p < 0.01$). In other words, if the personal photo is ephemeral (*versus persistent*), the participants perceived fewer concerns regarding personal data collection and dissemination. The results reflect the key advantages of ephemerality—being non-traceable and non-shareable. In essence, ephemeral sharing grants a limited time (e.g., five seconds) for viewing the picture and does not permit secondary access to the picture, thereby reducing the senders' data-related privacy concerns. Therefore, the functionality purges the possibility that the data could be tracked, saved, or disseminated by the receiver, which effectively extenuates the privacy concerns regarding data collection and dissemination.

[6] We also used the PROCESS model given by Hayes (2017) as a robustness check, and the estimation produced consistent results.

Second, our results reveal that the ephemeral treatment does not alleviate the identity disclosure concerns but the identity abuse concerns. The pattern that emerges is that the path from ephemeral to identity disclosure concerns is insignificant ($\beta_{Ephemeral \rightarrow Identity\ Disclosure\ Concerns} = 0.096$, $p > 0.1$); the path from ephemeral to identity abuse concerns is significant and negative ($\beta_{Ephemeral \rightarrow Identity\ Abuse\ Concerns} = -0.278$, $p < 0.01$).

Instead of considering the insignificant path as being futile in protecting users' identity disclosure, we instead regard it as the beauty of ephemeral sharing. One of the key advantages of ephemeral sharing—compared with conventional privacy-enhancing designs, such as anonymity, showing part of the photos, or privacy control—is that ephemeral sharing does not prevent personal information from being disclosed. The disclosed personal information can still be viewed by the receiver, regardless of whether it is ephemeral. It is reasonable that the sender remains concerned regarding re-identification even when the photo, by its nature, is ephemeral. Nevertheless, as the receiver cannot save or disseminate the personal photo, the likelihood of their identity being abused becomes minuscule compared with the likelihood of identity abuse with a persistent photo. Then, we saw a reduction in identity abuse concerns in the ephemeral condition.

Third, the tests of direct and indirect effects further specify the mediation relationships. Table E5 reports the coefficient, *p*-value, and the 95% bias-corrected and accelerated confidence interval (CI) for both direct and indirect effects from ephemeral to self-disclosure intention, respectively. Specifically, the paths for the three indirect effects—*(a) Ephemeral → Data Collection Concerns→ Self-disclosure; (b) Ephemeral → Data Dissemination Concerns→ Self-disclosure,* and *(c) Ephemeral → Identity Abuse Concerns→ Self-disclosure*—are all significant; the 95% CIs do not include zero. Meanwhile, the other two paths—*Ephemeral → Self-disclosure* and *Ephemeral → Identity Disclosure Concerns → Self-disclosure*—are insignificant, and both 95% CIs include zero, thereby suggesting insignificant indirect effects.

Table E5. Direct and Indirect Effects from Ephemeral to Self-disclosure Intention

Path	***Coeff.***	***p-value***	***95% CI***
Ephemeral → Self-disclosure	-0.047	0.510	[-0.187, 0.091]
Ephemeral → Data Collection Concerns→ Self-disclosure	**0.064**	**0.063**	**[0.016, 0.158]**
Ephemeral → Data Dissemination Concerns→ Self-disclosure	**0.132**	**0.003**	**[0.060, 0.237]**
Ephemeral → Identity Disclosure Concerns → Self-disclosure	0.010	0.528	[-0.005, 0.068]
Ephemeral → Identity Abuse Concerns→ Self-disclosure	**0.065**	**0.065**	**[0.010, 0.147]**

Note: 95% of CIs are biased corrected and accelerated bootstrap intervals.

Alternative Explanations

Institutional Privacy Concerns. An alternative mechanism regarding the effect of ephemeral sharing on self-disclosure intention is the alleviation of institutional privacy concerns. As ephemeral sharing can potentially prevent online dating platforms from collecting and using user data, the sender will likely perceive fewer risks from the platform's data usage behavior. Then, ephemeral sharing elicits a higher level of intention to self-disclose through the mitigation of institutional privacy concerns. However, our analyses turn down this possibility. Neither the direct effect of the path *Ephemeral → Institutional Privacy Concerns* nor the indirect effect of path *Ephemeral → Institutional Privacy Concerns → Self-disclosure* were significant ($\beta_{Ephemeral \rightarrow Institutional\ Privacy\ Concerns} = 0.094$, $p > 0.1$, 95% CI $\in$ [-0.089, 0.290]; $\beta_{Ephemeral \rightarrow Institutional\ Privacy\ Concerns \rightarrow Self\text{-}disclosure} = -0.016$, $p > 0.1$, 95% CI $\in$ [-0.083, 0.007], respectively). This suggests that in the matchmaking process, wherein the voluntary disclosure of personal information occurs in social interactions, the functionality of ephemeral sharing is more relevant to concerns of the

other user's data behavior but not that of the platforms. By this token, we rule out the alternative mechanism of institutional privacy concerns.

Self-presentation Intention. Another potential mechanism is self-presentation intention, which refers to the user's intention to create a desired self to manage others' impressions of him/her (Goffman, 1959). Specifically, the ephemeral sharing design can lower users' self-consciousness in communication and make them less interested in presenting an ideal self (Xu et al. 2016). Accordingly, the ephemeral group could expect a lower level of self-presentation intention, which consequently sees a reduction in the self-disclosure intention. To eliminate this possibility, we included the self-presentation intention in the PLS-SEM model. As Figure E1 illustrates, albeit the significant path from self-presentation intention to self-disclosure intention ($\beta_{Self\text{-}presentation\ intention \rightarrow\ Self\text{-}disclosure\ intention} = 0.160$, $p < 0.05$), the model did not identify any significant effect of ephemeral sharing on the self-presentation intention ($\beta_{Ephemeral \rightarrow\ Self\text{-}presentation\ intention} = 0.013$, $p > 0.1$). In other words, ephemeral sharing does not affect the user's willingness to self-present, thereby making it an unlikely mechanism that bridges ephemeral sharing and self-disclosure intention.

More importantly, the results reflect the purpose of communication in the context of online dating. Users engage in online dating activities to connect with a possible romantic partner (Finkel et al. 2012). As self-presentation is a key lever in attracting potential partners, they have the incentive to create an ideal self rather than a real self in the early stage of social interaction (Sedgewick et al. 2017). Therefore, even when the senders can use ephemeral sharing ex-ante a match, their self-presentation intention does not swing to strategically secure a match.

Additional Test

Disturbing Content. A persistent finding in extant literature regarding ephemeral sharing in social media platforms is that it provokes more disturbing content, thereby deteriorating the receiver's impression of the sender (Hofstetter et al. 2017). Therefore, ephemeral sharing can worsen the match outcome and conversational engagement via the distribution of disturbing content. We measure the disturbing content with two items. The first item asks the participants to indicate how likely they are to upload a disinhibited photo when using the photo feature (1- "strongly disagree" to 7- "strongly agree"). The second question requests participants to select the likelihood of uploading an explicit photo in the matching request (1- "very unlikely" to 7- "very likely"). The measure exhibited appropriate internal consistency, reliability, and discriminant validity from the main constructs. Thereafter, we averaged the two items to construct a measure of disturbing content. Then, as expected, the pairwise *t*-test did not report any significant, systematic differences in the mean value of disturbing content ($p > 0.1$). The finding harmonizes with the result in Section 5.2.2.5. Toxic Disinhibition that ephemeral treatment does not change the likelihood that the attached photo includes explicit or nude content extracted from image learning techniques.

We conclude that ephemeral sharing in online dating platforms does not generate more disturbing content. The results also validate our suspicion that users of online dating platforms refrain from disclosing explicit content to secure a match with a prospective date. Since any disclosure of disturbing content can be associated with a negative self-image, users will not lower their guard even if they have the opportunity to do so.

References

Choi BC, Jiang Z, Xiao B, Kim SS (2015) Embarrassing exposures in online social networks: An integrated perspective of privacy invasion and relationship bonding. *Information Systems Research*, 26(4):675–694.

Cobb C, Kohno T (2017) How public is my private life? Privacy in online dating. *Proceedings of the 26th International Conference on World Wide Web*. (Perth, Australia), 1231–1240.

Ellison N, Heino R, Gibbs J (2006) Managing impressions online: Self-presentation processes in the online dating environment. *Journal of Computer-mediated Communication* 11(2): 415–441.

Fornell C, Larcker D F (1981) Structural equation models with unobservable variables and measurement

error: *Algebra and Statistics*.
Goffman E (1959) *The Presentation of Self in Everyday Life*. (Garden City, NY, USA): Anchor.
Goodhue D L, Lewis W, Thompson R (2012) Does PLS have advantages for small sample size or non-normal data? *MIS Quarterly*. 36(3): 981–1001.
Hair JF, Hult GTM, Ringle, CM, Sarstedt M (2022) *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)* (3e). (Sage, Thousand Oaks, CA): Sage.
Henseler J, Ringle CM, Sarstedt M (2015) A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science* 43(1):115–135.
Hofstetter R, Rüppell R, John LK (2017) Temporary sharing prompts unrestrained disclosures that leave lasting negative impressions. *Proceedings of the National Academy of Sciences* 114(45):11902–11907.
Jiang Z, Heng CS, Choi BC (2013) Research note—privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research* 24(3):579–595.
Kock N, Hadaya P (2018). Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. *Information Systems Journal* 28(1): 227–261.
Lien CH, Cao Y, Zhou X (2017) Service quality, satisfaction, stickiness, and usage intentions: An exploratory evaluation in the context of WeChat services. *Computers in Human Behavior* 68:403–410.
Lutz C, Ranzini G (2017) Where dating meets data: Investigating social and institutional privacy concerns on Tinder. *Social Media+ Society* 3(1):1–12.
Obada-Obieh B, Somayaji A (2017) Can I believe you? Establishing trust in computer mediated introductions. *Proceedings of the 2017 New Security Paradigms Workshop*. (New York, USA), 94–106.
Ozdemir ZD, Jeff Smith H, Benamati JH. (2017) Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems* 26(6): 642–660.
Sedgewick JR, Flath ME, Elias LJ (2017) Presenting your best self (ie): The influence of gender on vertical orientation of selfies on Tinder. *Frontiers in Psychology* 8:604.
Waldman AE. (2019) Law, privacy, and online dating:"Revenge porn" in gay online communities. *Law & Social Inquiry* 44(4):987–1018.
Xu B, Chang P, Welker CL, Bazarova NN, Cosley D (2016) Automatic archiving versus default deletion: What snapchat tells us about ephemerality in design. In *Proceedings of the ACM Conference on Computer Supported Cooperative Work and Social Computing* (San Francisco, California, USA), 1662–1675.
Zhang NA, Wang CA, Karahanna E, Xu Y (2022) Peer privacy concerns: Conceptualization and measurement. *MIS Quarterly* 46(1):491–530.

Table E6. Constructs, Definitions, and Measurements

Construct	*Definition*	*Item*
Self-disclosure Intention	Intention to upload a personal photo in a dating request	If I were a user of this online dating platform, I would want to upload a personal photo in my dating request (adapted from Hofstetter et al. 2017). I am willing to disclose my facial information when using this photo feature (adapted from Hofstetter et al. 2017).
Disturbing Content	The degree to which the shared personal photo includes explicit content	I will likely send a disinhibited personal photo when using this photo feature (self-developed). I will likely send an explicit personal photo when using this photo feature (self-developed).
Data Collection Concerns	Concerns that other users will collect the personal information	When using this photo feature, I am concerned that the other users will **save** my photo to others without my consent (adapted from Zhang et al. 2022). When using this photo feature, I am concerned that the other user will **collect too much** of my personal information from the photo (adapted from Jiang et al. 2013).
Data Dissemination Concerns	Concerns that other users will disseminate the personal information	When using this photo feature, I am concerned that the other users will **share** my photo with others without my consent (adapted from Ozdemir et al. 2017). When using this photo feature, I am concerned that the other use will **disseminate** my photo to others without my consent (adapted from Waldman 2019).
Identity Disclosure Concerns	Concerns that the focal user's real identity will be disclosed to other users from the shared personal information	When using this photo feature, I am concerned that my friends/acquaintances/colleagues will identify me through the photo (Cobb and Kohno 2017). When using this photo feature, it is embarrassing to be identified from a personal photo. (adapted from Choi et al. 2015).
Identity Abuse Concerns	Concerns that the other users will abuse the identity for illegal use from the shared personal information	When using this photo feature, I am concerned that the other user will steal my identity for scams and catfishing (Cobb and Kohno 2017). When using this photo feature, I am concerned that the other user will conduct illegal activities with the photo (Obada-Obieh and Somayaji 2017).
Institutional Privacy Concerns	Concerns about the potential misuse of personal information from the online dating platform	I am concerned that the online dating platform will track and analyze my photo to support the service when using this photo feature (Lutz and Ranzini 2017). I am concerned that the online dating platform will sell my photo to other platforms or data brokers when using this photo feature (Lutz and Ranzini 2017).
Self-presentation Intention	Intention to present an ideal self via the personal photo	I want to present an ideal self with a personal photo when using this photo feature (Ellison et al. 2006). I am willing to express an ideal myself through personal photos when using this photo feature (Ellison et al. 2006).

Appendix F. Heterogeneous Treatment Effect on Privacy Sensitivity

Table F1. Heterogeneous Treatment Effect using *ProfileFace*

Variable	***NumPhoto***	***NumFace***	***NumMatch***	***Ln(SumMsgFromReceiver)***
	(1)	(2)	(3)	(4)
Ephemeral	0.139***(0.014)	0.131***(0.013)	0.148***(0.048)	0.082***(0.020)
ProfileFace	0.286***(0.026)	0.243***(0.025)	0.373***(0.065)	0.220***(0.026)
Ephemeral × *ProfileFace*	-0.097**(0.040)	-0.063*(0.038)	-0.212**(0.090)	-0.122***(0.037)
Controls	Yes	Yes	Yes	Yes
Constant	-0.532***(0.105)	-0.582***(0.103)	0.759***(0.195)	1.277***(0.087)
Observations	70,275	70,275	70,275	70,275
F test	62.52***	58.71***	548.03***	987.60***

Notes: Robust standard errors are given in parentheses; *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$