

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

Yumei He,^a Xingchen Xu,^b Ni Huang,^{c,*} Yili Hong,^c De Liu^d

^aA.B. Freeman School of Business, Tulane University, New Orleans, Louisiana 70118; ^bMichael G. Foster School of Business, University of Washington, Seattle, Washington 98195; ^cMiami Herbert Business School, University of Miami, Coral Gables, Florida 33146; ^dCarlson School of Management, University of Minnesota, Minneapolis, Minnesota 55455

*Corresponding author

Contact: yhe17@tulane.edu,  <https://orcid.org/0000-0002-8853-508X> (YuH); xcxu21@uw.edu,  <https://orcid.org/0000-0001-7269-4409> (XX); nhuang@miami.edu,  <https://orcid.org/0000-0003-3416-513X> (NH); khong@miami.edu,  <https://orcid.org/0000-0002-0577-7877> (YiH); deliu@umn.edu,  <https://orcid.org/0000-0002-9430-9732> (DL)

Received: July 21, 2021

Revised: February 3, 2023;
December 10, 2023

Accepted: January 9, 2024

Published Online in Articles in Advance:
March 11, 2024

<https://doi.org/10.1287/isre.2021.0379>

Copyright: © 2024 INFORMS

Abstract. Users on online dating platforms tend to encounter a cold-start problem, with limited user engagement in the initial stages of the matching process; this is partially due to privacy concerns. In this study, we propose ephemeral sharing as a privacy-enhancing design to strike a balance between users' privacy concerns and the need for voluntary information disclosure. Ephemeral sharing refers to a digital design in which the information shared (e.g., a personal photo) becomes invisible and irretraceable to the receiver shortly after the receipt of such information. In partnership with an online dating platform, we report a large-scale randomized field experiment with more than 70,000 users to understand how ephemeral sharing influences users' disclosure of personal photos, match outcome, and receiver engagement. The experiment features a treatment group in which subjects can upload an ephemeral photo along with their matching request and a control group in which subjects can instead upload a persistent photo. We find that users in the treatment group send more personal photos (and ones with human faces) compared with users in the control group. Additionally, the ephemeral sharing treatment leads to a higher number of matches and a higher level of receiver engagement. Further analyses suggest that the treatment effects are more salient for privacy-sensitive senders. Moreover, we find that the treatment effects on match outcome and receiver engagement can be explained by increases in the disclosure of personal photos. Last, through an online experiment, we show that ephemeral sharing increases disclosure intention by reducing privacy concerns related to data collection, dissemination, and identity abuse. Our study contributes to the literature and practice on privacy-enhancing designs for online matching platforms.

History: Alessandro Acquisti, Senior Editor; Beibei Li, Associate Editor.

Supplemental Material: The online appendix is available at <https://doi.org/10.1287/isre.2021.0379>.

Keywords: **ephemeral sharing • privacy-enhancing design • information disclosure • cold-start problem • online dating • randomized field experiment**

"... market participants want and need to preserve some privacy. Failure to give them enough privacy can make the market unsafe, which in turn can make it fail."

—Alvin E. Roth, *Who Gets What—and Why*, 2015

1. Introduction

In recent years, online dating platforms—such as *Bumble*, *Tinder*, and *Coffee Meets Bagel*—have become important avenues for individuals to find dating partners. A primary function of online dating platforms is to help users match with their potential dating partners and facilitate initial communication between them.¹ As

online dating trends are at an all-time high, individuals resort to virtual first dates before further pursuing relationships offline.² It has been reported that almost 40% of young people meet their partners online, and globally, the number of online dating users is estimated to exceed 441.8 million by 2024 (Rosenfeld et al. 2019, Statista 2020).

A key challenge related to online dating platforms is the cold-start problem (Chen 2021), wherein a sender may withhold personal information in the early stages of the matching process (Cobb and Kohno 2017), thereby making it difficult for the two parties to connect and communicate with each other.³ For example, many users exclude photos of themselves and/or other personal information from their profiles, such as height,

profession, or sexual orientation (Hall et al. 2010, Lutz and Ranzini 2017, Shi and Viswanathan 2023). Consequently, their matching requests may be regarded as inauthentic or untrustworthy, thereby undermining their likelihood of securing a match (John et al. 2016). Moreover, a lack of disclosure of personal information also makes it difficult for matched pairs to remain engaged after the initial match (Bapna et al. 2016, Jung et al. 2019).

A lack of personal information disclosure is partially due to users' privacy concerns—concerns regarding how user data could be used by companies, governments, or others (Jiang et al. 2013). Privacy concerns are also prevalent in online dating—Users may feel wary of their personal information and identity being disseminated, stolen, or abused, for example, used for scams and catfishing (Cobb and Kohno 2017). Furthermore, leaked personal information may also jeopardize a user's personal safety (Roth 2015). Consequently, users often hold back their personal information at least in the early phases of matching. However, the lack of disclosure of personal information due to privacy concerns hinders trust-building in early social interactions, and subjects for conversation become limited, thereby potentially impeding postmatch engagement. Unfortunately, according to regulations such as GDPR (General Data Protection Regulation), platforms in general cannot mandate disclosure of personal information (Aridor et al. 2020). Therefore, there is an acute need for novel platform designs that encourage voluntary disclosure of personal information without significantly compromising users' privacy protection.

Our study proposes and tests a privacy-enhancing self-disclosure mechanism—ephemeral sharing—to alleviate the cold-start problem in online dating. With ephemeral sharing, the content (e.g., personal photos) shared by a sender becomes invisible and irretraceable shortly after being revealed to the designated receiver (Xu et al. 2016). Compared with other privacy-enhancing designs—such as blurring, partially showing photos, or allowing users more control over information visibility (Keith et al. 2014, Tucker 2014)—ephemeral sharing enables unfettered sharing of information but severely restricts receivers' ability to store, disseminate, and misuse the information received. Although ephemeral sharing has been used in social media platforms, such as *Snapchat*, its application in online dating is new and provides novel opportunities for impacting not merely users' willingness to share (Vaterlaus et al. 2016, Hofstetter et al. 2017) but also tangible outcomes such as matches and the level of conversational engagement, which are the focus of this study. In addition, given the nuances of privacy concerns across contexts and the context-specific effectiveness of privacy interventions in assuring privacy (Acquisti et al. 2016, 2020), it is important to empirically examine how ephemeral

sharing can ease privacy concerns and thereby encourage personal information disclosure in online dating. Accordingly, we seek to address the following research questions:

(1) How does a privacy-enhancing ephemeral sharing design affect personal information disclosure behavior, match outcome, and postmatch engagement in online dating?

(2) What are the potential mechanisms underlying the effect of the ephemeral sharing design on personal information disclosure?

It is notable that we focus on how ephemeral sharing affects the matchmaking outcomes of strangers seeking romantic relationships, wherein the cold-start problem is salient. This differentiates our work from related prior studies on the ephemeral sharing design, which primarily focused on the communication behavior among socially connected users (Vaterlaus et al. 2016, Xu et al. 2016, Bayer et al. 2020). Theoretically it is unclear how ephemeral sharing impacts match outcomes in online dating. On the one hand, by encouraging self-disclosure, ephemeral sharing may reduce information asymmetry, foster trust among strangers, and facilitate the matching process. On the other hand, ephemeral sharing may lead to the revelation of unfavorable, disinhibited content, possibly leaving a negative impression on the receivers (Hofstetter et al. 2017). Moreover, as ephemeral sharing is integrated to enhance user privacy, it is theoretically meaningful to explore the mechanisms on how ephemeral sharing influences users' matching behaviors, particularly in terms of addressing different kinds of privacy concerns.

To answer these research questions, we report a large-scale randomized field experiment in partnership with Summer, a leading online dating platform. The experiment uses a between-subjects design at the user (the sender of the matching request) level with two groups: A treatment group that comprises senders who can upload *ephemeral* photos, and a control group where senders can upload *persistent* (i.e., nonephemeral) photos. The experimental manipulation occurs at the matching request stage, wherein senders in both groups can decide whether to include a photo in their matching requests. We then observe the users' initiation behaviors, match outcomes, and conversational engagement.

Our results reveal a series of notable findings. First, users in the treatment (*ephemeral*) group send a greater number of personal photos and photos that depict a human face, compared with users in the control group. Additionally, these users secure more matches and a higher level of conversational engagement from receivers (hereafter also referred to as receiver engagement), as measured by the number of messages received. Next, we explore the mechanisms underlying these effects. Our sequential mediation test suggests that the

observed effects of ephemeral sharing on the number of matches and receiver engagement are fully explained by the increase in the sender's disclosure of personal photos. To further evaluate that the effects are privacy-related, we conducted an online experiment that reveals that ephemeral sharing effectively reduces the sender's privacy concerns, especially about data collection, data dissemination, and identity abuse. We also ruled out alternative explanations, suggesting that neither benign nor toxic disinhibition, which is often associated with ephemeral sharing, was responsible for the observed effects. Finally, we explore the heterogeneous treatment effects. Our tests reveal that ephemeral sharing is more effective for privacy-sensitive senders—that is, those who opted not to include human faces in their user profiles. Last, we conducted a series of additional analyses to rule out other explanations such as treatment novelty and changes in photo content.

This study contributes to the literature on privacy management in online matching platforms (Tavani and Moor 2001, Acquisti et al. 2015) by proposing and testing a novel privacy-enhancing design—ephemeral sharing—to encourage personal information disclosure. Our design differs from other privacy-enhancing designs, for example, user privacy controls, in that ephemeral sharing is designed to encourage the sharing of personal information rather than hinder it. Our findings reveal that the ephemeral sharing improves information sharing by striking a balance between user privacy and voluntary disclosure of personal information. Second, our paper extends the extant literature on ephemeral sharing by examining the effects of ephemeral sharing on match outcomes, including the number of successful matches and the level of receiver engagement. Previous research on ephemeral sharing primarily focuses on sharing between already-connected users, whereas our setting begins with the sharing that takes place between two strangers. Existing research focuses more on the effect of ephemeral design on content-sharing behavior (Vaterlaus et al. 2016, Bayer et al. 2020), whereas our investigation extends to the downstream effects, including the number of matches and receiver engagement.

Furthermore, our research also provides actionable, practical implications for online matching platforms. We show that the ephemeral sharing design can be effective in mitigating the cold-start problem and improving receiver engagement in postmatch conversations. Therefore, managers of online matching platforms can encourage users to disclose personal information via ephemeral sharing or personalize users' information sharing design per their privacy sensitivity, such that users can use this design to achieve more matches and a higher level of engagement. After the experiment, the platform we collaborated with rolled out the ephemeral sharing mechanism to all users.

2. Literature Review and Conceptual Background

2.1. Online Dating

Our research belongs to a stream of studies that examines various issues in the online dating market including (a) the value of online dating, (b) assortative mating in dating preferences, and (c) the design of online dating platforms. In the first substream, research has established that online dating can accelerate the process of marriage (Rosenfeld 2017), improve marital satisfaction, and reduce break-ups (Cacioppo et al. 2013). The addition of mobile dating applications further enhances the value of online dating platforms (Jung et al. 2019). With regard to the second substream, prior research reveals that users of online dating platforms prefer prospective partners with similar traits (Hitsch et al. 2010a, b; Taylor et al. 2011). Furthermore, researchers have identified several assortative mating attributes, such as social desirability (Bruch and Newman 2018), attractiveness (Jia et al. 2015), and education (Whyte et al. 2018). This study belongs to the third substream. The literature on this substream has explored various design issues on online dating platforms, such as premium subscriptions (Yu et al. 2018), choice structure (Fong 2020, Jung et al. 2022), popularity scoring (Bojd and Yoganarasimhan 2022), demand information disclosure (Huang et al. 2022), performance feedback (Shi and Huang 2019), and verification (Shi and Viswanathan 2023). Our research adds to this substream by examining a novel ephemeral sharing design to promote personal information disclosure while protecting users' privacy, which is crucial for matching success.

2.2. Privacy Management

Ephemeral sharing can be considered a tool for privacy management, which broadly refers to the processes and activities that aim to protect users' personal information (Tavani and Moor 2001). The literature on privacy management can be grouped into three main categories: (a) economics of privacy, (b) design of privacy controls, and (c) privacy-enhancing technologies and designs (PETs) (Acquisti et al. 2016, 2020).

The first substream focuses on users' privacy decision making and the tradeoff between privacy and the benefits of information disclosure (Adjerid et al. 2016, 2019). A series of studies have explored how users trade their privacy for various economic gains, including lower prices and greater access to an application (Kummer and Schulte 2019), payments in the data-sharing market (Bergemann and Bonatti 2019), and other small financial incentives like a pizza (Athey et al. 2018, Lin 2022). Knowing that user data can be valuable for targeting and business value creation (Ghose et al. 2019), this literature also reveals that people may forgo their privacy for societal benefits, such as social adjustment benefits

(Lu et al. 2004), social awareness (Lowry et al. 2011), and social rewards (Jiang et al. 2013).

The second substream concerns the design of privacy controls. Several types of privacy control designs are explored in the literature, including default choice design, that is, opt-in versus opt-out (Lin 2022), framing design, that is, reject versus accept format (Samat and Acquisti 2017, Adjerid et al. 2018), timing of presenting privacy-control questions, that is, before versus after payment (Burtsch et al. 2015), and privacy seals and assurances (Rifon et al. 2005, Hui et al. 2007). Privacy controls examined in the literature tend to reduce personal information disclosure (Tsai et al. 2011), except for Wang et al. (2011), who use the reversibility design (i.e., the option to subsequently revise or retract the shared information) to encourage users' willingness to disclose information (Peer and Acquisti 2016).

Our research belongs to the third substream of literature on PETs, which refers to "technical and organizational mechanisms aiming to protect personal identity" (Burkert 1997, p. 125). Most PETs aim to conceal users' identity, the content of communication, and/or behavioral traces (Goldberg 2007, Borisov and Goldberg 2008, Heurix et al. 2015, Steed et al. 2022). Despite their significant role in protecting user identity, those PETs (e.g., encryption, anonymity, and pseudonymity) decrease the availability of personal information (Acquisti et al. 2016), which can hurt the market efficiency of online matching platforms (Bapna et al. 2016). In privacy-sensitive contexts, such as online dating, the users are reluctant to voluntarily disclose personal information; however, such personal information is critical to foster engagement in the initial matching stages. Therefore, our study contributes to the body of work on PETs by examining a privacy-enhancing design known as

ephemeral sharing, which motivates users to disclose personal information with privacy intact.

2.3. Ephemeral Sharing

2.3.1. Ephemeral Sharing on Social Media Platforms.

Initiated on social media platforms such as Snapchat, ephemeral sharing refers to the digital design that indicates that shortly after a piece of information is shared with an individual, the information will vanish and be no longer retrievable (Xu et al. 2016). The extant research has examined whether and how ephemeral sharing influences information-sharing behaviors. Ephemeral sharing may facilitate online disinhibition, a phenomenon of people saying and doing things online that they would not say or do in face-to-face settings (Suler 2004). Studies have revealed that ephemeral sharing may facilitate *toxic disinhibition*, leading to more toxic, excessive, and inappropriate self-disclosure, such as explicit content (Hofstetter et al. 2017), negative emotions, and cyberbullying (Utz et al. 2015, Vaterlaus et al. 2016). There is also evidence that ephemeral sharing facilitates *benign disinhibition*, which refers to positive, unconstrained self-expressions, such as more emotional, funny, and informal content (Xu et al. 2016), as well as a more congruent manner and better expression of their emotions (Vaterlaus et al. 2016). Additionally, ephemeral sharing facilitates informal conversations (Xu et al. 2016), playful interaction, and gratification (Waddell 2016, Phua et al. 2017, Saunders and Eaton 2018, Haber 2019).

There are differences in how ephemeral sharing is used in social media and online dating contexts, however, as detailed in Table 1. Prior literature has considered ephemeral sharing a digital design to support communication among users of social media platforms (Bayer et al. 2020). The goal of ephemeral sharing on

Table 1. Comparison of Ephemeral Sharing in Social Media and Online Dating Contexts

Aspect of Comparison	Social media	Online dating
Who uses ephemeral sharing?	Between already-connected users (Piwek and Joinson 2016, Vaterlaus et al. 2016, Phua et al. 2017)	Between strangers seeking romantic partners
In what ways does ephemeral sharing enhance social relationships?	Maintain existing relationships (Bayer et al. 2016, Waddell 2016)	Facilitate new relationships (i.e., matchmaking)
How does ephemeral sharing encourage self-disclosure?	Ephemeral sharing primarily mitigates self-presentation concerns (Bayer et al. 2016, Waddell 2016, Xu et al. 2016, Choi and Sung 2018, Wakefield and Wakefield 2018, Choi et al. 2020, Zhang et al. 2022b).	Enhancing privacy while increasing personal information sharing
What are the outcomes of interest for ephemeral sharing in this context?	Few studies have empirically supported that ephemeral sharing mitigates privacy concerns (Hofstetter et al. 2017).	Information disclosure in initial matching stages; Match outcomes, postmatch conversational engagement
	Information sharing (Poltash 2012, Vaterlaus et al. 2016, Hofstetter et al. 2017, Wakefield and Wakefield 2018, Yu and Riddle 2022)	

social media platforms is to maintain relationships by allowing already-connected users to express themselves in front of families, friends, or acquaintances (Bayer et al. 2016, Piwek and Joinson 2016, Vaterlaus et al. 2016, Waddell 2016, Phua et al. 2017). Prior research suggests that it primarily helps to ease self-presentation concerns, allowing for more genuine self-expression (Bayer et al. 2016). In contrast, online dating platforms involve romantic relationship formulation, with the goal of facilitating matchmaking between strangers (Finkel et al. 2012), thereby making information disclosure and trust-building critical in the initial interaction stages (Sedgewick et al. 2017). Therefore, in the context of online dating, ephemeral sharing functions as a privacy management tool that potentially lowers privacy barriers during initial interactions. Given the nuances of privacy concerns across contexts and the context-specific impact of privacy interventions in assuring privacy (Acquisti et al. 2016, 2020), it is important to empirically examine whether and how ephemeral sharing eases privacy concerns in online dating.

2.3.2. Ephemeral Sharing as a Privacy-Enhancing Digital Design in Online Dating. Building on the related literature, we propose that ephemeral sharing can serve as a privacy-enhancing design that addresses the cold-start problem in privacy-sensitive settings such as online dating. In online dating, users are expected to reveal personal information and interact with prospective dates who are strangers, and accordingly, privacy risks arise for users. We conceptualize users' concerns regarding risks such as social privacy concerns, which refers to user's negative feelings about potential privacy risks originating from the boundary regulations involved in social interactions (Altman 1976, Petronio 1991, Petronio 2002, Acquisti et al. 2022, Zhang et al. 2022a).

According to prior literature and our user interviews, we find that social privacy concerns in online dating comprise four components—that is, privacy concerns regarding data collection, data dissemination, identity disclosure, and identity abuse (further details are provided in Online Appendix A). Given that personal information such as photos is rather sensitive, it is reasonable to expect that many users do not want their data being stored on other users' devices and disseminated to a third party. Meanwhile, we also expect that identity-related privacy concerns are pronounced in online dating. For example, for online dating users, it might be embarrassing to be recognized by others who are offline friends, acquaintances, or coworkers (Cobb and Kohno 2017). Moreover, given that other users are typically strangers and may not even respond to matching requests, users are wary of identity-related misuse (Fiore et al. 2010). Their self-disclosed identities might be subject to identity abuse, such as identity

theft, catfishing, and other scams (Lutz and Ranzini 2017, Obada-Obieh and Somayaji 2017).

Bearing in mind the discussion on user social privacy concerns, it is notable that initial interactions are crucial for online dating, as a majority of the dating engagement ends at this stage (Finkel et al. 2012). Given the lack of verbal and nonverbal cues, during the initial interaction stages, users must seek to build trust with their prospective dates, which could lead to further engagement and relationship developments (Hallam et al. 2018). However, a direct outcome of the social privacy concerns in the online dating context is that users tend to withhold their personal information, such as their photos, during the initial interaction stage. When personal information is withheld, the prospective date likely perceives the other user as untrustworthy and assumes the worst about them (John et al. 2016). Without someone taking the first step in disclosing sensitive personal information, the likelihood of ensuing engagement decreases dramatically, thereby leading to failed matches not because the two parties are not a good fit for each other but driven by the cold-start problem (Obada-Obieh and Somayaji 2017, Hallam et al. 2018).

The ephemeral sharing design we propose addresses the cold-start problem by reducing users' social privacy concerns, thereby increasing users' disclosure of personal information during the initial interaction stage and leading to a greater number of matches. With ephemeral photos in the users' match request stage, the nature of automatic disappearance and the accompanying technology (e.g., blocking the ability to download or take screenshots) deters the receivers' permanent access to the shared photos.⁴ Therefore, in comparison with a persistent photo that can potentially be downloaded and reused by the receiver, the ephemeral photo temporarily connects the sender and receiver, but it disappears after a short period, setting them apart again, thereby avoiding potential personal boundary turbulences in the form of privacy violations (Teutsch et al. 2018). For example, ephemeral sharing significantly reduces the likelihood and mitigates the senders' concern that the shared personal information will be downloaded or disseminated by the receiver. As the receiver is only able to view the photo for a short period, the likelihood of misusing the photo for any repugnant activities is also significantly reduced. Therefore, the sender maintains ownership of personal information, thus preserving privacy. In other words, a sender who sends an ephemeral photo (compared with a regular, persistent photo) perceives a lower level of social privacy concerns for the shared photo; therefore, the sender is more likely to attach a personal photo with identity-revealing cues, such as the face, in the matching request.

The disclosure of personal information in the initial interaction stage of online dating—in our case, a personal

photo—reduces uncertainty and increases utility for prospective dates who are generally risk-averse. This unsolicited piece of sensitive information sends a positive signal to the receiver. For example, the action of disclosing personal photos could lead the receiver to associate the sender with desirable traits, such as trustworthiness, confidence, and open-mindedness (John et al. 2016). Moreover, the receiver might attribute the disclosure to the sender's genuine intention of relationship development (Petronio 1991) and be more likely to have a pleasant interaction. Moreover, a sender's initiation of information-sharing also reduces the barrier for the receiver to engage, as the receiver no longer needs to take the first step in disclosing their personal information. The reduced uncertainty for the prospective date also creates a sense of intimacy and liking, which is essential in dating (Berger and Calabrese 1974). Thus, the receiver is likely more willing to move forward from the initial interactions to learn more about the sender. Accordingly, we expect that the increased disclosure from the sender will lead to a higher probability of the match request being approved and further user engagement from the receiver.

In summary, based on our theorization of the ephemeral sharing design in the privacy-sensitive online dating context, we expect that by reducing users' social privacy concerns, the ephemeral sharing design at the match requesting stage would likely influence users' personal information disclosure, which leads to changes in the match outcome and conversational engagement, thereby addressing the cold-start problem in the initial phase of the matching process. Next, we present the experimental examination of ephemeral sharing in online dating.

3. Randomized Field Experiment

3.1. Research Context

We report a randomized field experiment in collaboration with Summer, a leading online dating platform that primarily serves users from East Asia (hereafter referred to as "the platform"). The platform uses a matching mechanism called Q&A-based matching, which is illustrated in Figure 1. Specifically, each user can list several open-ended screening questions on their matching request page, which are answered by senders as part of their matching requests. Popular screening questions may pertain to senders' dating preferences (e.g., Are you looking for a casual or a long-term relationship?), hobbies (e.g., What is your favorite song?), and plans (e.g., Where do you want to live in the future?). These questions are displayed on the user's profile page. When senders initiate a matching request, they share with the receiver answers to the receiver's screening questions, along with their profile information and possibly a personal photo (a feature

introduced in this experiment). The receiver is then notified of the matching request and decides whether to approve the matching request. If the request is approved by the receiver, the two users become *matched*. The sender and the receiver can then chat with each other using the integrated messaging tool in the platform's mobile application.

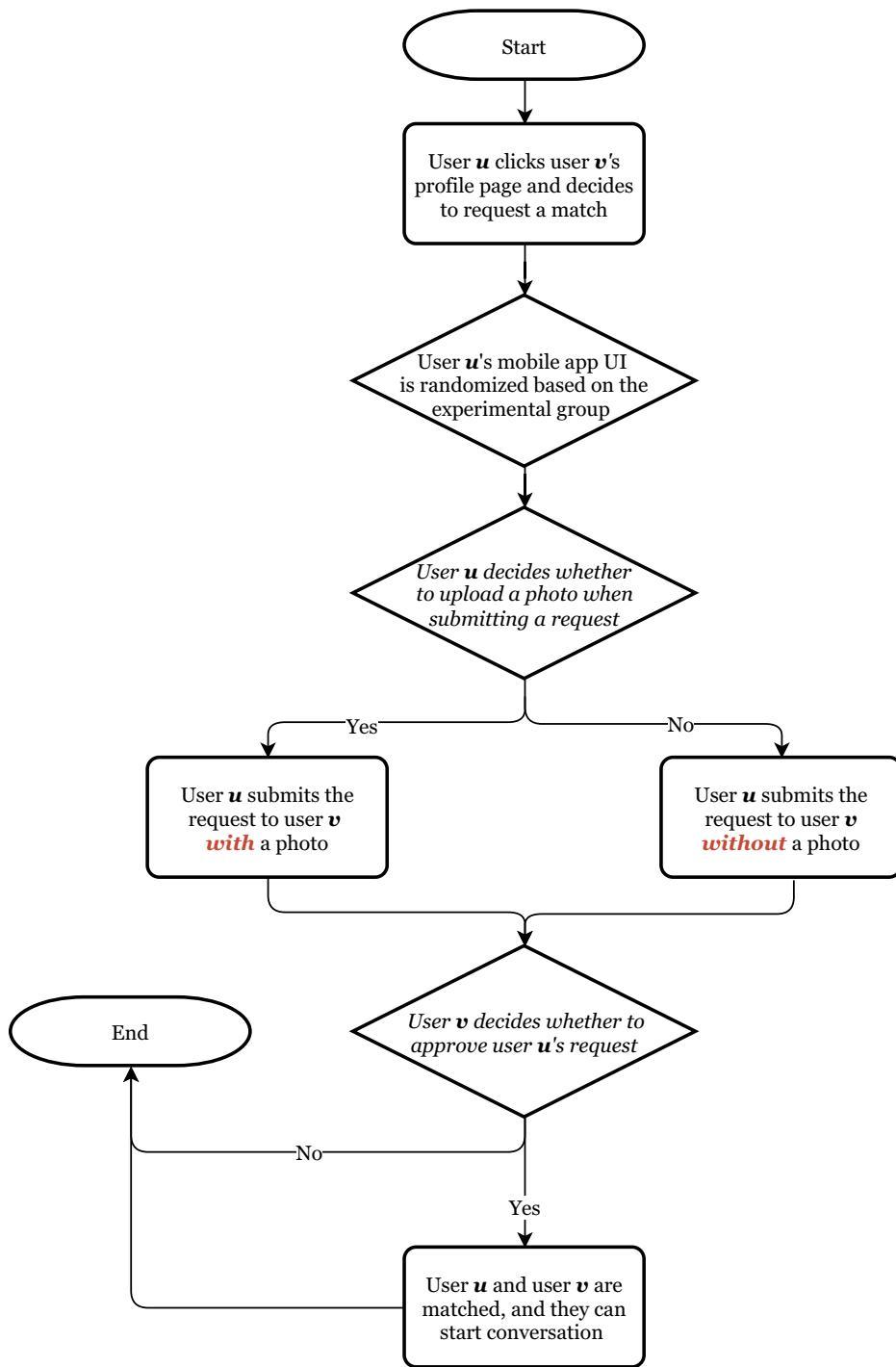
3.2. Experimental Design and Procedure

Our randomized field experiment used a user (sender)-level between-subjects design. The platform randomly assigned the users to either the treatment (comprising those who can upload ephemeral photos) or the control groups (comprising those who can upload persistent photos) as they updated the mobile application to Version 3.8.2 during this period; users stayed in the same group throughout the experiment. The experiment was implemented by the platform between February 28, 2020, and March 16, 2020, lasting 18 days, and no other experiments were running on the platform during this period. Besides, the platform moderated the posts in the mobile application's online community to ensure that our treatment was not discussed among users.

To ensure that users understood our treatment, the platform conducted extensive interviews and pilot tests with users of the platform, which confirmed that users adequately understood the concept of an ephemeral photo and the corresponding stimuli. Specifically, our experimental treatment encompasses several stimuli on the user interface (UI) for matching requests. First, on the matching request page (the page with the screening questions), as depicted in Figure 2, the treatment group has a photo-upload button that says "Upload a personal photo (ephemeral)," while the control group has a button that says "Upload a personal photo." Second, as Figure 3 illustrates, we vary the pop-up photo-upload dialogue page—which appears after a user taps the photo-upload button—in three ways: (a) The treatment UI mentions "Upload an ephemeral photo," whereas the control UI mentions "Upload a photo"; (b) the image for the treatment UI is one of the photos being burned, whereas the control UI does not (ephemeral is commonly known as "burn after viewing" in East Asian culture); and (c) compared with the control UI, the treatment UI includes an additional sentence explaining how the ephemeral photo functions.

Users are always allowed to post personal pictures on their profiles, either as their profile pictures or on their photo walls. Approximately 30% of the users have a profile picture with a human face, and 25% of photo walls have at least one picture with a human face. Our experiment is independent of the pictures in the user profiles and instead revolves around allowing senders to share a personal photo (either ephemeral or persistent) when sending a matching request. In addition, the

Figure 1. (Color online) Process Chart for a Matching Process



options of persistent and ephemeral photos were introduced into the production system simultaneously.

4. Data

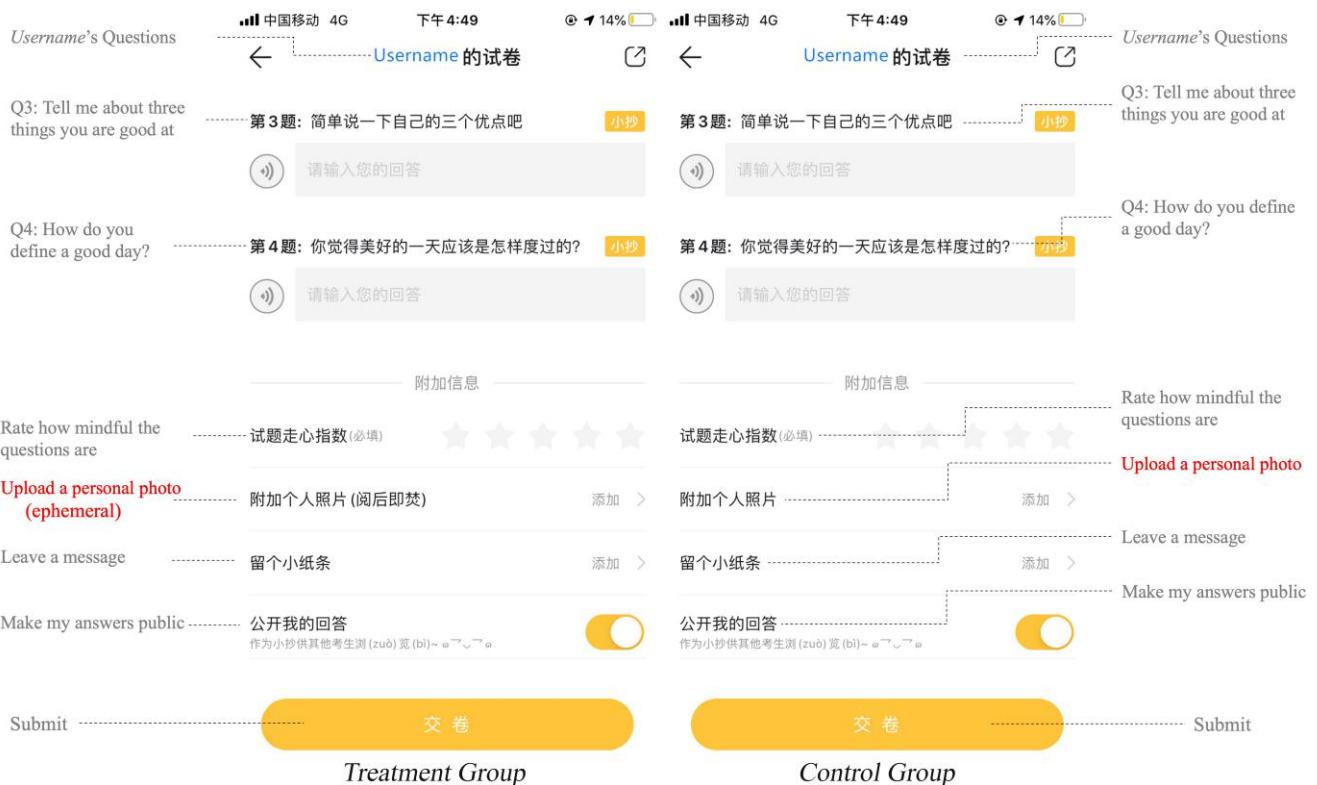
4.1. Data and Variables

We collected data from four different sources. First, we extracted experimental group assignments from the randomization system. Second, we retrieved users'

demographic and matching request information from the transactional database. Third, we obtained the users' tap-stream events from a cloud data warehouse for event logs. Last, we collected postmatch communication data from a third-party cloud data warehouse. In addition, we deidentified user data before extraction.

Aligning with the experimental design and level of analysis, we aggregated the behavioral trace data to

Figure 2. (Color online) Screenshot of the Request Page



Notes. Screenshot of the request page with manipulation information. The left image is the treatment UI for the matching request page, and the right image is the control UI for the corresponding page.

the user (sender) level and merged them with demographic information and group assignment. Tables 2 and 3 report the description and descriptive statistics of our variables, respectively. In particular, the following are the outcome variables of interest: the number of matching requests with a photo attached (*NumPhoto*), the number of photos that depict a human face (*NumFace*), the number of matches (*NumMatch*), and the number of messages from the receiver (*NumMsgFrom-Receiver*). The former two measures capture a user's information disclosure behavior. We used *NumPhoto* to denote photo-based self-disclosure. Such photos may or may not include a user's face, which is highly sensitive and important information regarding the user in online dating. We used *NumFace* to further capture the disclosure of highly privacy-sensitive information.⁵ Furthermore, we measured the variable *NumFace* using the face-detection API given by Baidu AI, a state-of-the-art face-detection API⁶; the reported precision of the service is above 99%. We also manually labeled 400 random images in terms of whether a human face is included in the image, and the face detection service provided accurate results for 395 of them, thereby resulting in a precision of 98.75%. The third measure, *NumMatch*, is a key match outcome, as a successful match is an important step toward developing a romantic relationship (Bapna

et al. 2016). The fourth outcome variable, *NumMsgFromReceiver*, represents the number of messages the subject has received from new connections, thereby measuring conversational engagement. Conversational engagement is important in online dating platforms (Jung et al. 2022) and it effectively captures the mitigation of the cold-start problem.

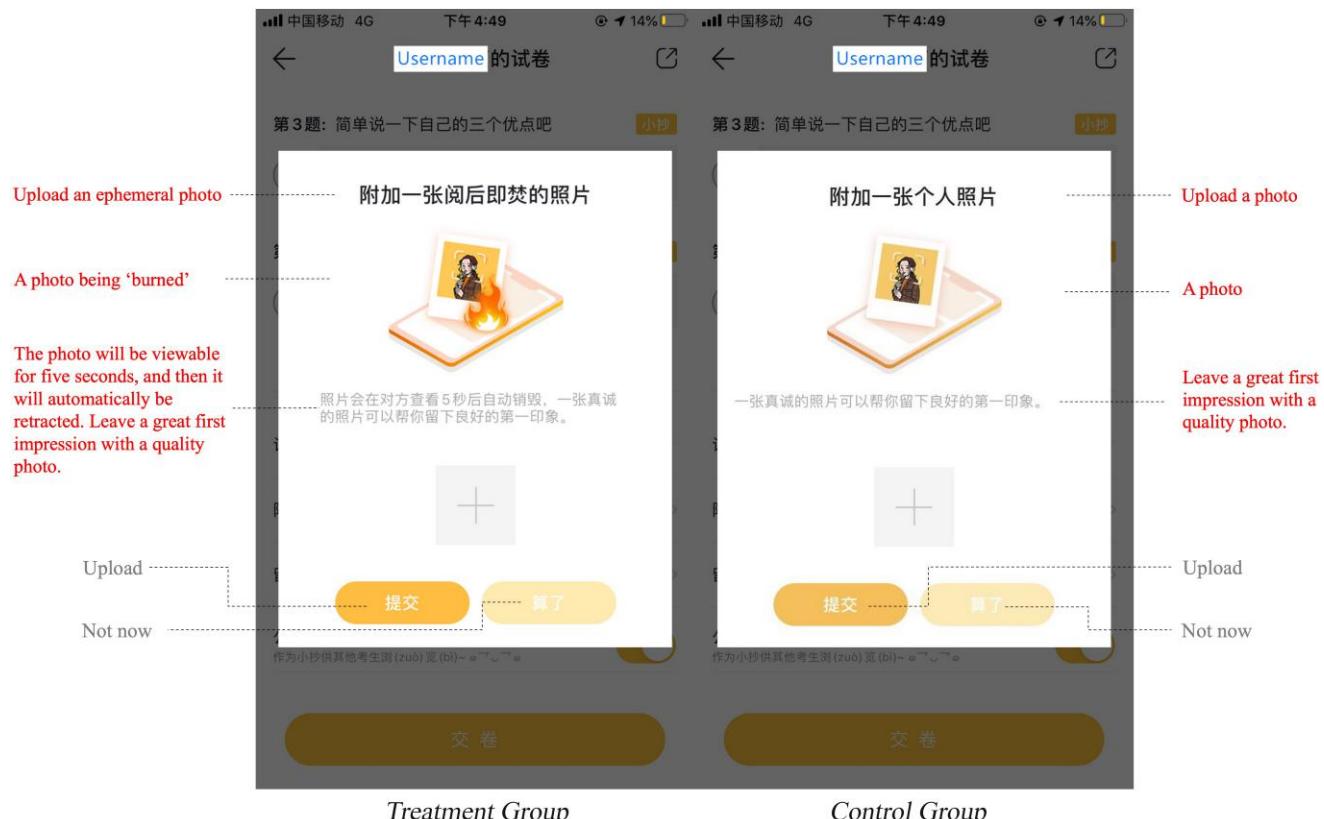
4.2. Randomization Checks

Before conducting formal analyses, we performed randomization checks on observed covariates across the two groups. As indicated in Table 4, pairwise *t* tests on numerical variables (profile face, photo wall face, gender, age, education, popularity, tenure, and enter date) and Kolmogorov-Smirnov tests on categorical variables (province, school, and major) indicate that there are no significant differences across the groups at conventional levels. Thus, the subjects were adequately randomized.

4.3. Model Specification

Equation (1) illustrates our main estimation equation, with the following dependent variables: $Outcome_u$ being the number of matching requests with photo (*NumPhoto*), the number of photos with faces (*NumFace*) shared by subject u , the number of matches (*NumMatch*), and the messages subject u received from the matches

Figure 3. (Color online) Screenshot of the Popup on the Request Page



Notes. Screenshot of the popup window after a user taps “upload a photo.” The left image is the treatment UI, and the right image is the control UI.

in which u served as the sender ($\text{SumMsgFromReceiver}$), respectively. The treatment indicator is $Ephemeral_u$, which indicates whether subject u was assigned to the ephemeral group. The equation also includes a series of covariates. The first covariate we include is the user's privacy sensitivity, proxied by whether the subject's photo wall includes a human face (PhotoWallFace). Our estimation also captures the effects of gender, age, education, and user popularity, as those attributes play a significant role in online dating preferences (Hitsch et al. 2010a, b; Taylor et al. 2011; Bruch and Newman 2018; Whyte et al. 2018). We also control for tenure as it affects application use behavior. Notably, for all the analyses in Section 5.1, model-free mean comparisons (via t tests) generate consistent results. Furthermore, there might be the potential unobserved effect of time when users enter the experiment. For example, users who update the application during the weekends might have more leisure time to explore the new feature. Therefore, we added a series of date dummies denoting the "enter date" in separate estimations.

$$Outcome_u = \beta_0 + \beta_1 Ephemeral_u + \boldsymbol{\beta} \text{ Control Variables}_u + \epsilon_u \quad (1)$$

5. Data Analyses and Results

5.1. Main Analyses

5.1.1. Effect of Ephemeral Sharing on Information Dis-

Closure Behavior. First, we explore the effect of ephemeral sharing on users' information disclosure behavior, in terms of the number of photos shared and the number of photos shared that include human faces. Table 5 reports the results of OLS estimations.⁸ First, columns (1) and (2) report the effects of ephemeral sharing on the number of photos shared, without and with controlling for the enter date dummies, respectively. The estimated coefficients of *Ephemeral* in the two models are both significant and positive ($\beta_{Ephemeral} = 0.111, p < 0.01$). The average number of photos shared in the control group is 0.215 and the effect size of 0.111 corresponds to a relative increase of 52.1%, which is economically significant. Second, the effect of ephemeral treatment on *NumFace*, as shown in columns (3) and (4), is also significant ($\beta_{Ephemeral} = 0.113, p < 0.01$). This is a relative increase of 61.6% in the number of photos with human faces. Taken together, the results in Table 5 suggest that ephemeral sharing increases users' disclosure of privacy-sensitive personal information.⁹

Table 2. Variable Descriptions of the User-Level Data

Variable	Description
Treatment <i>Ephemeral</i>	Whether the subject received the ephemeral treatment (0 = Persistent, 1 = Ephemeral).
User demographics <i>ProfileFace</i>	A binary variable that indicates whether a human face is shown in the profile (0 = Without human face, 1 = With human face).
<i>PhotoWallFace</i>	A binary variable indicating whether the sender has photos that include human faces on his/her photo wall (0 = Without human face, 1 = With human face).
<i>Gender</i>	A binary gender indicator (0 = Female, 1 = Male).
<i>Age</i>	A numerical integer that captures a subject's age.
<i>Education</i>	The education level of a subject (0 = High school or below, 1 = bachelor's degree, 2 = Master's degree, 3 = Doctoral degree).
<i>Popular</i>	Whether the subject has an above-median popularity score (0 = below-median or unpopular, 1 = above-median or popular). ⁷
<i>Tenure</i>	The subject's tenure since registration (in days).
<i>EnterDate</i>	The day when a subject joined the experiment (the date when our experiment began, defined as Enter Date 1).
Behavioral data at the user level	
<i>NumRequestPageView</i>	The number of matching request pages that a subject viewed during the experiment.
<i>NumRequest</i>	The number of matching requests that a subject sent during the experiment.
<i>NumPhoto</i>	The number of matching requests with a photo attached that a subject sent during the experiment.
<i>NumFace</i>	The number of matching requests with a photo that includes a human face that a subject sent during the experiment.
<i>NumMatch</i>	The number of matching requests that a subject sent and were accepted during the experiment
<i>SumMsgFromReceiver</i>	The total number of messages that a subject received from matches initiated by him/her during the experiment.

5.1.2. Effect of Ephemeral Sharing on the Match Outcome. Next, we turn to the effects of ephemeral sharing on the match outcome. Table 6 presents that the users in the treatment group achieve more matches than those in the control group ($\beta_{\text{Ephemeral}} = 0.086$ and 0.079, respectively, both $p < 0.05$). This translates into an increase of 3.3% in the number of matches. Therefore, ephemeral sharing does improve matching for users.

5.1.3. Effect of Ephemeral Sharing on the User Engagement Outcome. To examine whether ephemeral sharing can alleviate the cold-start problem, we consider receiver engagement, operationalized as the number of total messages from the receivers of match requests (*SumMsgFromReceiver*). We log-transformed *SumMsgFromReceiver*, as its distribution is highly skewed. The results in Table 7 indicate that users in the treatment

Table 3. Descriptive Statistics of the User-Level Data

Variable	Observations	Mean	Standard deviation	Minimum	Maximum
User demographics					
<i>ProfileFace</i>	70,275	0.302	0.459	0	1
<i>PhotoWallFace</i>	70,275	0.250	0.433	0	1
<i>Gender</i>	70,275	0.623	0.485	0	1
<i>Age</i>	70,275	24.223	2.615	19	32
<i>Education</i>	70,275	1.371	0.652	0	3
<i>Popular</i>	70,275	0.500	0.500	0	1
<i>Tenure</i>	70,275	282.144	221.607	1	1,027
Behavioral data at the user level					
<i>NumRequestPageView</i>	70,275	14.954	34.857	1	1,302
<i>NumRequest</i>	70,275	5.877	12.225	0	160
<i>NumPhoto</i>	70,275	0.271	1.975	0	128
<i>NumFace</i>	70,275	0.242	1.857	0	128
<i>NumMatch</i>	70,275	2.769	5.566	0	109
<i>SumMsgFromReceiver</i>	70,275	112.761	334.957	0	10,031

Table 4. Randomization Checks

Numerical variables	t value	p value
<i>ProfileFace</i>	1.383	0.167
<i>PhotoWallFace</i>	0.043	0.966
<i>Gender</i>	1.477	0.140
<i>Age</i>	0.375	0.707
<i>Education</i>	-0.543	0.588
<i>Popular</i>	-0.026	0.979
<i>Tenure</i>	0.745	0.456
<i>EnterDate</i>	-0.973	0.331
Categorical variables	Combined K-S	p value
<i>Province</i>	0.005	0.716
<i>School</i>	0.008	0.240
<i>Major</i>	0.004	0.954

group accrued more messages from receivers ($\beta_{Ephemeral} = 0.045$ or 0.042 , $p < 0.05$). The results suggest that the matches in the treatment group produced 4.6% more messages from the receivers of match requests meant for the request senders than those in the control group. The increase in postmatch conversations suggests that ephemeral sharing can effectively alleviate the cold-start problem.¹⁰

5.2. Mechanisms

Having estimated the total effects of ephemeral sharing on the outcomes of interest, we next attempt to understand the underlying mechanisms. We began by testing a set of “behavioral” mechanisms—that is, whether the effects of ephemeral sharing were due to increased personal information disclosure and/or alternative mechanisms. Our tests confirmed the former mechanism and ruled out several alternatives. Next, we further investigate why ephemeral sharing leads to increased disclosure of personal photos using an online experiment. We describe these mechanism explorations and findings here.

5.2.1. Mediation Effect of Information Disclosure Behavior.

One mechanism in which ephemeral sharing can lead to more matches (*NumMatch*) and receiver engagement ($Ln(SumMsgFromReceiver)$) is by increasing the number of photos uploaded. Ephemeral sharing can reduce users’ privacy concerns, thereby making them more willing to upload personal photos in their matching requests. Subsequently, receivers might find such requests more trustworthy and are thus more likely to accept the requests and engage in conversations with such senders. To test this mechanism, we used both *NumPhoto* and *NumMatch* as mediators. The two mediators are sequential because matches are prerequisites to messages. Since our mediation model includes two mediators in a sequence, we used a sequential mediation analysis that considers four key variables that occur in sequence, *Ephemeral*, *NumPhoto*, *NumMatch*, and $Ln(SumMsgFromReceiver)$, with earlier variables possibly affecting the subsequent ones. There can be a total of four paths from *Ephemeral* to $Ln(SumMsgFromReceiver)$: (1) *Ephemeral* → *NumPhoto* → *NumMatch* → $Ln(SumMsgFromReceiver)$, (2) *Ephemeral* → *NumPhoto* → $Ln(SumMsgFromReceiver)$, (3) *Ephemeral* → *NumMatch* → $Ln(SumMsgFromReceiver)$, and (4) *Ephemeral* → $Ln(SumMsgFromReceiver)$.

We conducted the sequential mediation analyses using the PROCESS Model with 5,000 bootstrap samples (Hayes 2017). Figure 4 depicts two significant paths: Path (1)—*Ephemeral* → *NumPhoto* → *NumMatch* → $Ln(SumMsgFromReceiver)$ —has a 95% confidence interval (CI) of [0.011, 0.021] that does not include zero, which suggests that the ephemeral treatment sequentially increases the number of matching requests with photos, the number of matches, and the number of messages received. In addition, Path (2)—*Ephemeral* → *NumPhoto* → $Ln(SumMsgFromReceiver)$ —also has a 95% CI [0.0001, 0.004] that does not include zero. Combining results from Paths (1) and (2), it appears that disclosing

Table 5. Regression Results for *NumPhoto* and *NumFace*

Variable	<i>NumPhoto</i>		<i>NumFace</i>	
	(1)	(2)	(3)	(4)
<i>Ephemeral</i>	0.111*** (0.015)	0.111*** (0.015)	0.113*** (0.014)	0.113*** (0.014)
<i>PhotoWallFace</i>	0.145*** (0.019)	0.144*** (0.019)	0.131*** (0.018)	0.130*** (0.018)
<i>Gender</i>	0.245*** (0.014)	0.233*** (0.014)	0.229*** (0.013)	0.220*** (0.013)
<i>Age</i>	0.023*** (0.005)	0.023*** (0.005)	0.025*** (0.005)	0.025*** (0.005)
<i>Education</i>	-0.044** (0.019)	-0.046** (0.019)	-0.039** (0.017)	-0.041** (0.017)
<i>Tenure</i>	-2E-4*** (3E-5)	-2E-4*** (3E-5)	-2E-4*** (3E-5)	-2E-4*** (3E-5)
<i>Popular</i>	0.142*** (0.017)	0.119*** (0.018)	0.125*** (0.016)	0.106*** (0.017)
<i>Constant</i>	-0.487*** (0.103)	-0.354*** (0.113)	-0.546*** (0.100)	-0.443*** (0.108)
Observations	70,275	70,275	70,275	70,275
EnterDate dummies	No	Yes	No	Yes
F test	59.84***	18.99***	58.97***	18.79***

Note. Robust standard errors are given in parentheses.

*** $p < 0.01$; ** $p < 0.05$; * $p < 0.1$.

Table 6. Regression Results for *NumMatch*

Variable	<i>NumMatch</i>	
	(1)	(2)
Ephemeral	0.086** (0.041)	0.079** (0.040)
<i>PhotoWallFace</i>	0.184*** (0.047)	0.162*** (0.047)
Gender	1.232*** (0.046)	1.042*** (0.045)
Age	0.003 (0.009)	0.001 (0.009)
Education	-0.062 (0.039)	-0.089** (0.038)
Tenure	-0.001*** (9E-5)	-0.001*** (9E-5)
Popular	2.957*** (0.046)	2.585*** (0.043)
Constant	0.820*** (0.195)	3.168*** (0.222)
Observations	70,275	70,275
EnterDate dummies	No	Yes
F test	625.54**	233.20***

Note. Robust standard errors are given in parentheses.

*** $p < 0.01$; ** $p < 0.05$; * $p < 0.1$.

personal photos not only increases the number of matches and the number of receiver messages (indirectly through the number of matches), but directly increases the number of receiver messages as well. Furthermore, Paths (3) and (4) are not significant, thereby suggesting that the ephemeral sharing feature does not directly lead to more matches or postmatch engagement, but exerts such effects through increasing disclosure of personal information. Replacing *NumPhoto* with *NumFace* yields identical results (Online Appendix B).

5.2.2. Alternative Mechanisms

5.2.2.1. Number of Request Page Views and Matching Requests. The ephemeral design may increase a user's number of request pageviews or matching requests as alternative mechanisms. In other words, the senders in the treatment group—after learning about the option of sending an ephemeral photo—could possibly change their decision on how many request pages to view and how many matching requests to send.

Table 7. Regression Results for *Ln(SumMsgFromReceiver)*

Variable	<i>Ln(SumMsgFromReceiver)</i>	
	(1)	(2)
Ephemeral	0.045*** (0.017)	0.042** (0.017)
<i>PhotoWallFace</i>	0.109*** (0.020)	0.098*** (0.019)
Gender	0.244*** (0.019)	0.149*** (0.019)
Age	0.003 (0.004)	0.002 (0.004)
Education	0.013 (0.016)	0.001 (0.016)
Tenure	-5E-4*** (4E-5)	-6E-4*** (4E-5)
Popular	1.529*** (0.018)	1.337*** (0.018)
Constant	1.312*** (0.087)	2.295*** (0.093)
Observations	70,275	70,275
EnterDate dummies	No	Yes
F test	1,118.07**	468.27***

Note. Robust standard errors are given in parentheses.

*** $p < 0.01$; ** $p < 0.05$; * $p < 0.1$.

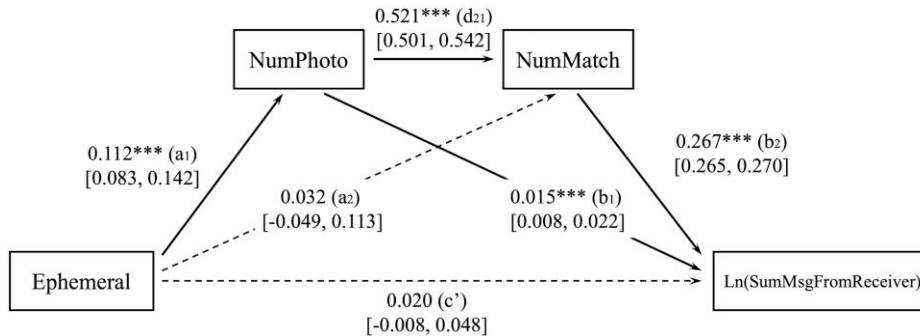
Therefore, we estimate whether there are significant differences across the two groups in terms of (1) the number of request pages browsed (*NumRequestPageView*), and (2) the number of matching requests sent (*NumRequest*). As Table 8 reports, there are no significant differences in *NumRequestPageView* ($p > 0.1$) or *NumRequest* ($p > 0.1$).

5.2.2.2. Choice of Prospective Receivers. It could also be that the ephemeral photo feature leads the senders to select different kinds of prospective dates, which could also affect match outcomes. For example, they may be emboldened by the ephemeral photo feature to pursue a more popular or higher-quality partner. Conversely, they may pursue a more diverse set of prospective dates. For each sender who made at least one matching request during the experiment, we calculated the average age, education level, tenure, and popularity of the receivers pursued by the sender. Meanwhile, when there were at least two matching requests, we calculated the standard deviations of these measures. Table 9 presents the descriptions of variables, and Table 10 reports the descriptive statistics and the results of *t* tests for group comparisons. The *t* tests suggest no significant differences between the two groups in terms of receiver age, education, tenure, or popularity, which rule out the possibility that the effects were due to shifts in users' choice of prospective dates.

5.2.2.3. Treatment Novelty. The results could potentially be explained by novelty effects that users may have abnormally strong interests in the feature when it was first introduced, which may lead to more photo-sharing and better match outcomes. To test this possibility, we divided the time between a user's entry into the experiment and the end of the experiment (Day 18) into two time windows (T_1 and T_2). For example, if a user updated the app on the third day of our experiment, we counted Day 3 to Day 10 as T_1 (eight days) and the remaining days as T_2 (eight days). A significant decay in the treatment effects in T_2 would indicate a strong novelty effect. Hence, we reanalyzed the data by adding an interaction term between *Ephemeral* and T_2 , which captures the decay in the treatment effect. The regression results in Table 11 reveal no significant interaction effects. Specifically, the estimated coefficients of *Ephemeral* $\times T_2$ for *NumPhoto*, *NumFace*, *NumMatch*, and *Ln(SumMsgFromReceiver)* are all insignificant ($\beta = -0.014$, $\beta = -0.011$, $\beta = -0.000$, and $\beta = -0.012$, respectively, with $p > 0.1$). Therefore, we conclude that treatment novelty was not likely at play during our experiment.

Apart from the previous alternative mechanisms, it is also likely that ephemeral sharing resulted in different content of photos being shared (as opposed to the number of personal photos being shared) that lead to

Figure 4. Sequential Mediation Analysis Using *NumPhoto* and *NumMatch* as Mediators



Note. Estimated indirect effects (Hayes 2017): $a_1 \rightarrow d_{21} \rightarrow b_2$: 0.016, 95% CI $\in [0.011, 0.021]$; $a_1 \rightarrow b_1$: 0.002, 95% CI $\in [0.0001, 0.004]$; $a_2 \rightarrow b_2$: 0.009, 95% CI $\in [-0.013, 0.031]$.

different match outcomes and conversational engagement. Here, we identify whether the characteristics of shared photos could explain our findings. Specifically, we investigate three aspects of the content: benign disinhibition, toxic disinhibition, and facial attractiveness.

5.2.2.4. Benign Disinhibition. Extant literature on ephemeral sharing suggests that ephemeral sharing might facilitate benign disinhibition in online settings, which refers to positive, unconstrained self-expressions, such as openly sharing personal experiences, opinions, and emotions (Joinson 1998, Suler 2004). Benign disinhibition has more to do with emotional safety than privacy concerns; For example, a private setting may not be safe for people to relax and freely display their emotions and vice versa. Increased benign disinhibition alone could likely lead to more disclosure and the development of a new relationship (Vaterlaus et al. 2016). To test the possibility, we follow Hofstetter et al. (2017) and Xu et al. (2016) to examine facial attributes for clues of benign disinhibition. Specifically, we leveraged multiple computer

vision methods to detect signs of benign disinhibition from the faces shared by users, including whether the faces displayed a neutral emotion, appeared synthetic, and were straight. We posit that a user was more benignly disinhibited, if the faces they shared were less emotionally neutral, less synthetic, and less straight. Table 12 explains the measures of (reverse-coded) benign disinhibition (more details in Online Appendix C).

If benign disinhibition plays a significant role, we would expect the photos in the treatment group to be different from those in the control group in terms of the benign disinhibition measures. However, as indicated in Table 13, none of the pairwise t tests is significant, thereby suggesting that benign disinhibition is not at play.

5.2.2.5. Toxic Disinhibition. Extant literature on ephemeral sharing suggests that ephemeral sharing might facilitate toxic disinhibition in the online space, such as sharing of explicit or nude photos (Vaterlaus et al. 2016, Waddell 2016). To empirically test the possibility of this,

Table 8. Regression Results for *NumRequestPageView* and *NumRequest*

Variable	<i>NumRequestPageView</i>		<i>NumRequest</i>	
	(1)	(2)	(3)	(4)
<i>Ephemeral</i>	0.273 (0.257)	0.217 (0.250)	0.120 (0.089)	0.107 (0.088)
<i>PhotoWallFace</i>	1.342*** (0.320)	1.152*** (0.310)	0.422*** (0.105)	0.382*** (0.105)
<i>Gender</i>	10.909*** (0.284)	9.319*** (0.265)	4.786*** (0.095)	4.422*** (0.092)
<i>Age</i>	0.007 (0.059)	0.002 (0.058)	0.290*** (0.023)	0.286*** (0.023)
<i>Education</i>	0.492* (0.259)	0.229 (0.252)	-1.007*** (0.096)	-1.058*** (0.095)
<i>Tenure</i>	-0.002*** (6E-4)	-0.003*** (6E-4)	-0.004*** (2E-4)	-0.004*** (2E-4)
<i>Popular</i>	13.654*** (0.304)	10.604*** (0.277)	4.990*** (0.103)	4.273*** (0.100)
<i>Constant</i>	0.487 (1.267)	25.176*** (1.441)	-4.283*** (0.486)	0.146 (0.519)
<i>Observations</i>	70,275	70,275	70,275	70,275
<i>EnterDate dummies</i>	No	Yes	No	Yes
<i>F</i> test	319.97***	206.22***	476.24	177.93***

Note. Robust standard errors are given in parentheses.

*** $p < 0.01$; ** $p < 0.05$; * $p < 0.1$.

Table 9. Variable Descriptions Related to Pursued Receivers

Variable	Description
<i>Mean_Age</i>	The average age of the receivers that a focal subject sent matching requests to during the experiment.
<i>Mean_Education</i>	The average education level of the receivers that a focal subject sent matching requests to during the experiment.
<i>Mean_Tenure</i>	The average tenure of the receivers that a focal subject sent matching requests to during the experiment.
<i>Mean_Popularity</i>	The average popularity of the receivers that a focal subject sent matching requests to during the experiment.
<i>SD_Age</i>	The standard deviation of the age of the receiver that a focal subject sent matching requests to during the experiment.
<i>SD_Education</i>	The standard deviation of the education level of the receivers that a focal subject sent matching requests to during the experiment.
<i>SD_Tenure</i>	The standard deviation of the tenure of the receivers that a focal subject sent matching requests to during the experiment.
<i>SD_Popularity</i>	The standard deviation of the popularity of the receivers that a focal subject sent matching requests to during the experiment.

we leverage an explicit content classifier to extract two measures—the ratios of explicit and nude photos sent by the same sender (*Explicit%* and *Nude%*, with the former being more inclusive). Table 14 explains the measures (see Online Appendix C for more details)—the higher the ratio of explicit photos, the *more toxically disinhibited* a user is. If toxic disinhibition is at play, the photos in the treatment group will have a higher ratio of explicit/nude photos compared with those in the control group. Again, pairwise *t* tests suggest that the differences between the two groups in the abovementioned measures are insignificant (Table 15). The results here are consistent with our analysis of the user’s intention to disclose disturbing content in the online survey-based experiment in Online Appendix E, as the pairwise *t* test did not show any significant differences between the treatment and control groups in the mean value of the user’s intention of disclosing disturbing content ($p > 0.1$).

5.2.2.6. Facial Attractiveness. Another possible explanation of our findings is that ephemeral design leads to the sharing of more attractive photos. To rule out this alternative explanation, we focus on the facial attractiveness of the photos, the most accessible source of facial

information that affects the receiver’s match decision-making (Jia et al. 2015). We measure the facial attractiveness of each user who includes the face in the photo attached to the matching requests. To operationalize facial attractiveness, we build and train a TransFBP-based prediction model using a high-quality, crowd-sourced *Beauty Rating* data set on the platform (Xu et al. 2018). The comparisons between our model and the benchmark models indicate that our model performs as well as the state-of-the-art methods. Online Appendix D reports more details regarding the prediction process of facial attractiveness. Specifically, from all the photos sent by experimental subjects, we collect the photos including faces that are eligible for the facial attractiveness prediction model, and then predict the facial attractiveness score for each photo. Afterward, we average the score for all the photos sent by each subject to get a subject-level facial attractiveness score. The score ranges from 1 to 10; the higher the score, the more attractive the subject is. After we obtained the average score on facial attractiveness, we conducted a *t* test comparison of the average score of facial attractiveness between the two groups. The analysis reveals that the difference in scores between the ephemeral and persistent groups is statistically insignificant (Facial Attractiveness_{Ephemeral} = 5.823,

Table 10. Descriptive Statistics on Receivers Pursued and Results of the *t* Test

Variable	Treatment group		Control group		<i>t</i> test result	
	Mean	Standard deviation	Mean	Standard deviation	<i>t</i> value	<i>p</i> value
<i>Mean_Age</i>	23.809	2.000	23.816	1.994	-0.422	0.673
<i>Mean_Education</i>	1.358	0.475	1.364	0.476	-1.242	0.214
<i>Mean_Tenure</i>	271.968	151.705	271.629	151.240	0.250	0.803
<i>Mean_Popularity</i>	1.21E-5	1.52E-5	1.21E-5	1.50E-5	0.127	0.900
<i>SD_Age</i>	1.772	0.893	1.783	0.897	-1.212	0.225
<i>SD_Education</i>	0.409	0.289	0.414	0.290	-1.549	0.121
<i>SD_Tenure</i>	191.515	85.188	192.530	85.701	-1.140	0.254
<i>SD_Popularity</i>	9.14E-6	1.72E-5	9.16E-6	1.73E-5	-0.106	0.916

Table 11. Ruling Out Treatment Novelty Effect

Variable	NumPhoto (1)	NumFace (2)	NumMatch (3)	Ln(SumMsgFromReceiver) (4)
Ephemeral	0.062*** (0.007)	0.062*** (0.007)	0.040** (0.019)	0.041*** (0.015)
T_2	-0.000 (0.007)	-0.002 (0.006)	0.290*** (0.021)	0.138*** (0.015)
$Ephemeral \times T_2$	-0.014 (0.011)	-0.011 (0.011)	-0.000 (0.030)	-0.012 (0.021)
Controls	Yes	Yes	Yes	Yes
Constant	-0.177*** (0.042)	-0.221*** (0.040)	1.425*** (0.083)	1.632*** (0.059)
Observations	140,550	140,550	140,550	140,550
F test	31.93***	31.26***	388.01***	710.81***

Note. Robust standard errors are given in parentheses.

*** $p < 0.01$; ** $p < 0.05$; * $p < 0.1$.

Facial Attractiveness_{Persistent} = 5.818, $p = 0.750$). Thus, ephemeral sharing does not appear to indicate differences in senders' facial attractiveness.

5.3. Why Does Ephemeral Sharing Lead to More Personal Information Disclosure?

Our analyses has revealed that ephemeral sharing improves match outcomes and user engagement by increasing personal information disclosure. There are several potential explanations. Our hypothesis is that ephemeral sharing alleviates users' social privacy concerns related to their personal information being misused and disseminated and their identity being disclosed and abused by other users. An alternative explanation is that ephemeral sharing reduces their concerns that their personal information could be collected and abused by the platform, that is, *institutional privacy concerns* (Lutz and Ranzini 2017). Another explanation is that ephemeral sharing can empower and encourage the intention of self-representation (Xu et al. 2016). To narrow down the theoretical explanations, we conducted another online experiment to further understand the underlying mechanisms by which ephemeral sharing affects personal information disclosure intention (i.e., self-disclosure intention). We summarize the experimental setup and main findings below, with further details (e.g., participants recruitment, additional results, and diagnostics) provided in Online Appendix E.¹¹

5.3.1. Participants. We carried out the online experiment in China to be consistent with the setting of our randomized field experiment. A group of 105 individuals participated in the experiment at *Sojump*, a popular Qualtrics-like survey and experiment platform in Asia (Lien et al. 2017). All participants completed the experiment. The participants were either students whose educational backgrounds were similar to the users of our partner platform or professionals with experience in product design in leading digital platforms. We used a between-subjects design, with participants randomly assigned to either a treatment condition (the "ephemeral" condition, $n = 53$) or a control condition (the "persistent" condition, $n = 52$).

5.3.2. Procedure and Stimulus. On the landing page, the participants were told to try a newly launched attach-a-photo feature for an online dating platform. We asked participants to visualize a scenario in which they were to send a matching request to a prospective date. Each participant, depending on the assigned group, watched a video clip that demonstrated how to attach an ephemeral or persistent photo in a matching request (available upon request). The two video clips were identical except that they depicted an ephemeral and a persistent photo, respectively. After watching the video clip, the participants completed a questionnaire with items for constructs related to several possible theoretical mechanisms (e.g., social privacy concerns,

Table 12. Descriptions of Variables Proxying Benign Disinhibition (User Level)

Variable	Description
NeutralEmotion%	The ratio of faces with neutral emotion (including the faces that Baidu API cannot detect any emotion) to all the faces disclosed by a focal subject. The more emotionally neutral the subject is in the photo, the <i>less benignly disinhibited</i> the subject is.
Synthetic	The average synthetic score of all the faces disclosed by a focal subject. The synthetic score is between 0 and 1, with a higher value indicating the photo is more likely altered. the more synthetic the photo is, the <i>less benignly disinhibited</i> the subject is.
StraightFaced%	The ratio of straight faces to all the faces disclosed by a focal subject. The straighter the face is, the more formal the subject is in the photo and thus <i>less benignly disinhibited</i> .

Table 13. Descriptive Statistics and *t* Tests on Measures of Benign Disinhibition

Variable	Treatment group		Control group		<i>t</i> test result	
	Mean	Standard deviation	Mean	Standard deviation	<i>t</i> value	<i>p</i> value
NeutralEmotion%	0.546	0.478	0.539	0.481	0.524	0.600
Synthetic	7.4E-4	1.4E-3	7.4E-4	1.3E-3	0.002	0.999
StraightFaced%	0.797	0.389	0.795	0.391	0.221	0.826

institutional privacy concerns, self-representation intention), manipulation checks, attention checks, and demographics. Upon completing the task, each participant received a random reward worth between 1 and 2 dollars.

5.3.3. Instruments and Validation. To measure social privacy concerns, we adapted existing privacy scales to the online dating context. Specifically, we measured social privacy concerns in four dimensions—that is, privacy concerns regarding data collection, data dissemination, identity disclosure, and identity abuse. We also included constructs for alternative mechanisms—that is, institutional privacy concerns and self-presentation intention. All the constructs exhibited appropriate internal consistency, convergent validity, and discriminant validity (see Online Appendix E). We used the partial least squares structural equation modeling (PLS-SEM) to test the mechanisms (Jiang et al. 2013, Hair et al. 2022).¹²

5.3.4. Results. The estimations yield several key findings, as reported in Table 16 and Figure 5. First, ephemeral sharing significantly reduces three dimensions of social privacy concerns, data collection, data dissemination, and identity abuse concerns, but not identity disclosure concerns. These findings confirm the key advantages of ephemerality in preventing storage and further dissemination of shared personal data. Unlike some other privacy control designs, ephemeral design discloses personal information to the receiver and, thus, cannot prevent identity disclosure. Yet, because ephemeral design prevents the receiver from downloading or forwarding a personal photo, the likelihood of identity abuse is significantly reduced, thereby resulting in reduced identity abuse concerns. Second, mediation tests (Table 16) further confirm that data

collection, dissemination, and identity abuse concerns fully mediate the effect of ephemeral design on personal information disclosure intention. In contrast, institutional privacy concerns and self-representation intention were not impacted by ephemeral design, nor did they mediate the relationship between ephemeral design and disclosure intention. These findings suggest that ephemeral design indeed achieves the design goal of enhancing user privacy as a means of improving match outcomes.

5.4. Heterogeneous Treatment Effects: Privacy Sensitivity

We also aim to ascertain whether the ephemeral sharing feature affects certain users more than others. Given that ephemeral sharing alleviates social privacy concerns, we conjecture that those who are more sensitive to privacy concerns are affected more by this feature. In online dating platforms, privacy-sensitive users are more prone to withhold facial information from their “photo wall” (on which users can share photos of themselves—for example, of the food they cook, places they have traveled to, or their pets), as such facial photos may disclose their identity to other users of the platform. Overall, 25% of users uploaded photos that included human faces on their photo wall. Therefore, we proxy a user’s privacy sensitivity with a dummy variable *PhotoWallFace*, thereby indicating whether the user has uploaded any photo with a human face to his/her photo wall (1 = has a human face, 0 = no human face). To examine the effect of privacy sensitivity, we augmented our user-level analysis by adding an interaction term—*Ephemeral* × *PhotoWallFace*.

The results in Table 17 indicate negative interaction effects (*Ephemeral* × *PhotoWallFace*) on information disclosure behaviors, match outcome, and conversational engagement. Specifically, the estimated coefficients of

Table 14. Descriptions of Variables that Proxy for Toxic Disinhibition (User Level)

Variable	Description
Explicit%	The ratio of explicit photos to all the photos shared by a user. Explicit photos include photos classified as “porn,” “hentai,” or “sexy” by Baidu API.
Nude%	The ratio of nude photos to all the photos shared by a user. Nude photos include the photos classified as “porn” or “hentai” by Baidu API.

Table 15. Descriptive Statistics and *t* Tests for Measures of Toxic Disinhibition (User Level)

Variable	Treatment group		Control group		<i>t</i> test result	
	Mean	Standard deviation	Mean	Standard deviation	<i>t</i> value	<i>p</i> value
Explicit%	0.037	0.157	0.038	0.163	-0.344	0.731
Nude%	0.014	0.097	0.016	0.105	-0.950	0.342

Ephemeral \times *PhotoWallFace* for *NumPhoto*, *NumFace*, *NumMatch* and *Ln(SumMsgFromReceiver)* are all negative and significant ($\beta = -0.093$, $p < 0.05$; $\beta = -0.078$, $p < 0.05$; $\beta = -0.201$, $p < 0.05$; $\beta = -0.097$, $p < 0.05$, respectively). The findings suggest that the treatment effects on information disclosure behaviors, match outcomes, and conversational engagement are *more* pronounced for privacy-sensitive senders. In addition, we also conducted a robustness check with an alternative measure of privacy sensitivity using *ProfileFace*—that is, whether a human face is displayed in a user’s profile. The regressions yield similar results (see Online Appendix F). Therefore, ephemeral sharing is *more* effective for users who are sensitive to privacy, thereby suggesting its privacy-enhancing role.

6. Discussion

6.1. Main Findings

In online dating platforms, privacy concerns hold users back from voluntarily disclosing personal information that is valuable for mitigating the cold-start problem. To address this issue, our research proposed a privacy-enhancing design that allows a user to share a photo on an ephemeral basis with the matching request and tested its effect in a large-scale randomized field experiment. Our analysis of the experiment suggests that the ephemeral photo-sharing design, compared with persistent photo-sharing, improves the match outcome and postmatch conversational engagement. Moreover, our mediation analysis confirmed that the effects resulted from the increase in the sender’s disclosure of personal photos at the matching request stage. Furthermore, we ruled out multiple alternative explanations, such as treatment novelty effect, increase in matching requests, and shift in photo

content. To further understand the reasons behind the increased disclosure of personal photos, we conducted an online experiment that measured theoretical constructs such as users’ social privacy concerns, institutional privacy concerns, and self-presentation intention. The results suggest that the ephemeral design elevated self-disclosure intention by reducing social privacy concerns related to data collection, data dissemination, and identity abuse, but not identity disclosure, institution privacy concerns, and self-presentation intention. Finally, we found that the treatment effects of ephemeral sharing on information disclosure behaviors, match outcome, and receiver engagement were more pronounced among privacy-sensitive senders.

6.2. Contribution to the Literature

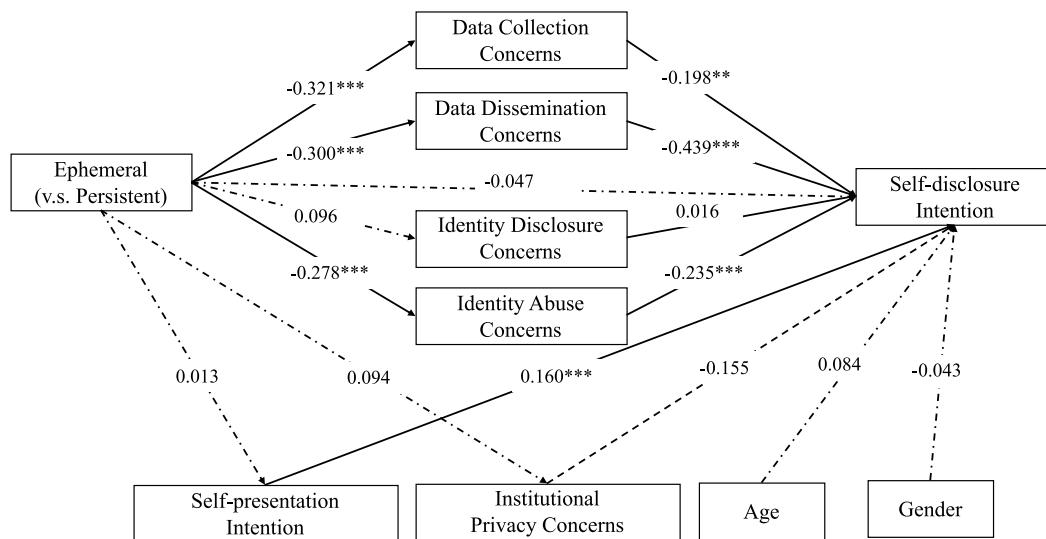
Our research makes several contributions to related literature. First, this study extends emerging research on privacy management—in particular, privacy-enhancing technologies and designs—to online matching platforms. Our paper is among the first to test a novel privacy-enhancing mechanism in online matching platforms for reducing users’ privacy concerns without holding back the disclosure of valuable personal information, which is in contrast with the approach of blocking information flow in the form of privacy control measures (Tucker 2014). The former approach is particularly important for contexts like online dating, in which disclosure of personal information is crucial, for example, for addressing the cold-start problem and maintaining a healthy engagement between users (Bapna et al. 2016). Furthermore, we demonstrated the privacy-enhancing effects of the ephemeral sharing design using a combination of objective data (disclosure behavior) and subjective measures of social privacy concerns. Our

Table 16. Direct and Indirect Effects from Ephemeral to Self-Disclosure Intention

Path	Coefficient	<i>p</i> value	95% CI
Ephemeral \rightarrow self-disclosure	-0.047	0.510	[-0.187, 0.091]
Ephemeral \rightarrow data collection concerns \rightarrow self-disclosure	0.064	0.063	[0.016, 0.158]
Ephemeral \rightarrow data dissemination concerns \rightarrow self-disclosure	0.132	0.003	[0.060, 0.237]
Ephemeral \rightarrow identity disclosure concerns \rightarrow self-disclosure	0.010	0.528	[-0.005, 0.068]
Ephemeral \rightarrow identity abuse concerns \rightarrow self-disclosure	0.065	0.065	[0.010, 0.147]

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

Figure 5. PLS-SEM Model Analyses



Note. * $p < 0.1$; ** $p < 0.05$; *** $p < 0.01$.

findings strongly support the effectiveness of the ephemeral sharing design in reducing social privacy concerns and promoting value-added personal information disclosure.

Next, our research also advances the stream of literature on ephemeral sharing. First, the extant literature about ephemeral sharing primarily suggests it as a means to maintain relationships for already-connected users in social media (Vaterlaus et al. 2016), whereas our study elucidates that, in an online dating context, ephemeral sharing facilitates matchmaking among strangers who wish to establish romantic relationships. Second, although prior research has revealed that ephemeral sharing design influences users' information-sharing behaviors on social media platforms (Choi and Sung 2018), our research extends the discussion that in the context of online matching platforms, ephemeral sharing can also impact downstream outcomes including match outcome and postmatch conversational engagement. Third, although prior literature posits that ephemeral

sharing primarily mitigates self-presentation concerns in social media context (Bayer et al. 2020), our research demonstrates that, within the context of online dating, ephemeral sharing enhances user privacy while increasing personal information sharing.

Last, our research also speaks to the literature on the value of personal information (Elvy 2017, Collis et al. 2021, Mehta et al. 2021). Related prior work indicates the realization of the value of personal information in digital platforms through data network effects (Acquisti et al. 2016, Ichihashi 2021, Acemoglu et al. 2022) in which firms extract the value of personal data through algorithmic tools such as recommendations (e.g., for matching purposes) (Gregory et al. 2021). Instead of feeding personal data to a recommendation system, our research showcases the role of users' voluntary sharing of personal information in peer-to-peer interactions. In this manner, the value of personal information was effectively realized by the users of the platform.

Table 17. Heterogeneous Treatment Effect Using *PhotoWallFace* for Interaction

Variable	NumPhoto (1)	NumFace (2)	NumMatch (3)	Ln(SumMsgFromReceiver) (4)
Ephemeral	0.134*** (0.016)	0.133*** (0.015)	0.136*** (0.046)	0.070*** (0.020)
<i>PhotoWallFace</i>	0.192*** (0.026)	0.170*** (0.024)	0.284*** (0.068)	0.157*** (0.028)
Ephemeral × <i>PhotoWallFace</i>	-0.093** (0.038)	-0.078** (0.036)	-0.201** (0.095)	-0.097** (0.040)
Controls	Yes	Yes	Yes	Yes
Constant	-0.499*** (0.103)	-0.555*** (0.100)	0.795*** (0.195)	1.300*** (0.088)
Observations	70,275	70,275	70,275	70,275
F test	54.42***	53.10***	547.43***	979.30***

Note. Robust standard errors are given in parentheses.

*** $p < 0.01$; ** $p < 0.05$; * $p < 0.1$.

6.3. Managerial Implications

Our research provides actionable implications for privacy-enhancing practices in digital platforms. First, online dating platforms or other privacy-sensitive settings can implement the ephemeral sharing design to encourage users to disclose personal information while largely preserving their privacy. It is significant that after the experiment ended, the platform integrated the feature into its production system and ephemeral sharing became a popular feature among users. Such privacy-enhancing features can be crucial for a variety of other online platforms on which the disclosure of personal information is essential, such as online health, online therapy, and online financial services. Second, although our ephemeral sharing design is tailored to photo-sharing, similar design patterns can be applied to other forms of private information, including text, audio, and video. Third, our results reveal that ephemeral sharing cannot regarding identity disclosure. A platform can devise other strategies that can mitigate identity disclosure concerns to further enhance user's privacy.

6.4. Limitations and Future Research

Our research is subject to several limitations. First, our research does not provide insights into how ephemeral sharing may impact the receiver's behaviors, which is a good direction for future research. Second, given the data limitation, we used the number of messages to measure conversational engagement; future research could further examine the textual content of such messages and offline engagement behaviors. Third, in our examination of the treatment heterogeneity, we find that users' responses to the ephemeral sharing design per privacy sensitivity. Inspired by Zhang et al. (2019), future research can further explore additional covariates that help the platform perform personalized and targeted information-sharing design. At last, it would be useful for future research to generalize our findings regarding ephemeral sharing to contexts other than online dating.

6.5. Conclusion

We aim to address an important issue in a privacy-sensitive setting, the cold-start problem, as users in online dating platforms typically refrain from disclosing their personal information during the initial interaction phases, thereby making it difficult for strangers to establish engagement and continue the process of romancing the other. In turn, we test a privacy-enhancing ephemeral sharing feature and show that ephemeral sharing encourages the disclosure of personal photos, which leads to a larger number of matches and further increases in user engagement, thereby effectively addressing the cold-start problem. User privacy and data protection are increasingly important in digital

platforms (Aridor et al. 2020). Our paper builds on prior work in the privacy literature, makes an initial effort in the online dating context, and calls for more privacy-enhancing designs for digital platforms. We hope that our study is part of the upcoming efforts to test and understand effective privacy-enhancing mechanisms.

Endnotes

¹ In a typical matching process, the user ("sender") sends a matching request to a preferred dating partner ("receiver") with some personal information; the receiver reviews the matching request and decides whether to accept it. If the receiver accepts it, the match is successful, and the two parties are able to further communicate with each other.

² See <https://www.npr.org/2021/07/20/1017962403/google-searches-for-dating-reached-5-year-high>.

³ In our paper, personal information refers to the information or opinion that directly or indirectly identifies a user referenced from the enactment of privacy regulations (e.g., the General Data Protection Regulation (GDPR), <https://gdpr.eu/eu-gdpr-personal-data/>). It is also called private information, personally identifiable information, or personal data.

⁴ Although technology disables common photo saving actions, such as downloading or taking screenshots, it does not prevent a receiver from taking a picture of the sender's shared photo with a separate device. However, we believe such cases are rare and the pictures taken are not in the original format or resolution.

⁵ We assume that the human face in the photo is the face of the subject who sends the matching request; thus, including a human face implies that the sender discloses his/her own real identity. First, our treatment message explicitly advocates that users upload personal photos. Second, and more importantly, users voluntarily disclose a face in the photo, and thus, they do not have the incentive to misrepresent another's face. Third, the sender and the receiver usually engage in offline meetings to find an ideal partner.

⁶ See <https://ai.baidu.com/ai-doc/FACE/yk37c1u4t>.

⁷ Following prior studies (Bruch and Newman 2018, Shi and Viswanathan 2023), we compute a user's popularity by first building a network based on connection requests and then applying the PageRank algorithm to compute the popularity score.

⁸ Although we adopt OLS regression for *NumPhoto*, *NumFace*, *NumMatch*, and *SumMsgFromReceiver* due to its ease of interpretation, our robustness checks using negative binomial models for these outcome variables yielded simulating findings.

⁹ The number of requests was not affected by the treatment (Table 7).

¹⁰ Our main analysis lands at the user level, which implies that we count all the requests for each sender. However, we also conduct robustness checks for the first request. The regressions on the first request yielded almost identical findings, respectively, using the likelihood of uploading a photo, including a human face in the photo, having a matching request approved, and receiving any receiver messages as outcomes of interest.

¹¹ Prior to the online experiment, we interviewed users of online dating platforms to understand their perceptions of ephemeral sharing and privacy concerns. We also conducted a pretest to validate the instruments and adjust the scales, which were used in the online experiment. Because of limitations of space, we omitted the details of the interviews and pretest (available upon request).

¹² We used the bootstrapping method with 1,000 iterations to generate the path coefficients. We also used the PROCESS model by Hayes (2017) as a robustness check, and the estimation yielded consistent results.

References

- Acemoglu D, Makhdoomi A, Malekian A, Ozdaglar A (2022) Too much data: Prices and inefficiencies in data markets. *Amer. Econom. J.: Microeconom.* 14(4):218–256.
- Acquisti A, Brandimarte L, Hancock J (2022) How privacy's past may shape its future. *Science* 375(6578):270–272.
- Acquisti A, Brandimarte L, Loewenstein G (2015) Privacy and human behavior in the age of information. *Science* 347(6221):509–514.
- Acquisti A, Brandimarte L, Loewenstein G (2020) Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *J. Consumer Psych.* 30(4):736–758.
- Acquisti A, Taylor C, Wagman L (2016) The economics of privacy. *J. Econom. Literature* 54(2):442–492.
- Adjerid I, Acquisti A, Loewenstein G (2019) Choice architecture, framing, and cascaded privacy choices. *Management Sci.* 65(5):2267–2290.
- Adjerid I, Peer E, Acquisti A (2018) Beyond the privacy paradox: Objective vs. relative risk in privacy decision making. *Management Inform. Systems Quart.* 42(2):465–488.
- Adjerid I, Acquisti A, Telang R, Padman R, Adler-Milstein J (2016) The impact of privacy regulation and technology incentives: The case of health information exchanges. *Management Sci.* 62(4):1042–1063.
- Altman I (1976) Privacy: A conceptual analysis. *Environ. Behav.* 8(1): 7–29.
- Aridor G, Che YK, Salz T (2020) The economic consequences of data privacy regulation: Empirical evidence from GDPR. Preprint, submitted January 29, <https://dx.doi.org/10.2139/ssrn.3522845>.
- Athey S, Catalini C, Tucker C (2018) The digital privacy paradox: Small money, small costs, small talk. Preprint, submitted February 15, <https://dx.doi.org/10.2139/ssrn.2916489>.
- Bapna R, Ramaprasad J, Shmueli G, Umyarov A (2016) One-way mirrors in online dating: A randomized field experiment. *Management Sci.* 62(11):3100–3122.
- Bayer JB, Triệu P, Ellison NB (2020) Social media elements, ecologies, and effects. *Annual Rev. Psych.* 71:471–497.
- Bayer JB, Ellison NB, Schoenebeck SY, Falk EB (2016) Sharing the small moments: Ephemeral social interaction on Snapchat. *Inform. Comm. Soc.* 19(7):956–977.
- Berger CR, Calabrese RJ (1974) Some explorations in initial interaction and beyond: Toward a developmental theory of interpersonal communication. *Human Comm. Res.* 1(2):99–112.
- Bergemann D, Bonatti A (2019) Markets for information: An introduction. *Annu. Rev. Econom.* 11:85–107.
- Bojd B, Yoganarasimhan H (2022) Star-cursed lovers: Role of popularity information in online dating. *Marketing Sci.* 41(1):73–92.
- Borisov N, Goldberg I (eds.) (2008) Privacy enhancing technologies. *Proc. 8th Internat. Sympos. on Privacy Enhancing Tech.* (Springer, Berlin), 5134.
- Bruch EE, Newman MEJ (2018) Aspirational pursuit of mates in online dating markets. *Sci. Adv.* 4(8):eaap9815.
- Burkert H (1997) Privacy-enhancing technologies: Typology, critique, vision. *Technology and Privacy: The New Landscape* (MIT Press, Cambridge, MA), 125–142.
- Burtsch G, Ghose A, Wattal S (2015) The hidden cost of accommodating crowd-funder privacy preferences: A randomized field experiment. *Management Sci.* 61(5):949–962.
- Cacioppo JT, Cacioppo S, Gonzaga GC, Ogburn EL, VanderWeele TJ (2013) Marital satisfaction and break-ups differ across on-line and off-line meeting venues. *Proc. Natl. Acad. Sci. USA* 110(25): 10135–10140.
- Chen A (2021) *The Cold Start Problem: How to Start and Scale Network Effects* (HarperCollins, New York).
- Choi TR, Sung Y (2018) Instagram vs. Snapchat: Self-expression and privacy concern on social media. *Telemation Inform.* 35(8): 2289–2298.
- Choi S, Williams D, Kim H (2020) A snap of your true self: How self-presentation and temporal affordance influence self-concept on social media. *New Media Soc.* 1–22.
- Cobb C, Kohno T (2017) How public is my private life? Privacy in online dating. *Proc. 26th Internat. Conf. on World Wide Web*, 1231–1240.
- Collis A, Moehring A, Sen A, Acquisti A (2021) Information frictions and heterogeneity in valuations of personal data. Preprint, submitted December 2, <https://dx.doi.org/10.2139/ssrn.3974826>.
- Elvy SA (2017) Paying for privacy and the personal data economy. *Columbia Law Rev.* 117(6):1369.
- Finkel EJ, Eastwick PW, Karney BR, Reis HT, Sprecher S (2012) Online dating: A critical analysis from the perspective of psychological science. *Psych. Sci. Public Interest* 13(1):3–66.
- Fiore AT, Taylor LS, Zhong X, Mendelsohn GA, Cheshire C (2010) Who's right and who writes: People, profiles, contacts, and replies in online dating. *Proc. 43rd Hawaii Internat. Conf. on System Sci.* (IEEE, Piscataway, NJ), 1–10.
- Fong J (2020) Effects of market size and competition in two-sided markets: Evidence from online dating. Preprint, submitted June 29, <https://dx.doi.org/10.2139/ssrn.3458373>.
- Ghose A, Li B, Liu S (2019) Mobile targeting using customer trajectory patterns. *Management Sci.* 65(11):5027–5049.
- Goldberg I (2007) Privacy-enhancing technologies for the Internet, III: Ten years later. Acquisti A, Gritzalis S, Lambrinoudakis C, di Vimercati S, eds. *Digital Privacy: Theory, Technologies, and Practices* (CRC Press, New York), 25–40.
- Gregory RW, Henfridsson O, Kaganer E, Kyriakou SH (2021) The role of artificial intelligence and data network effects for creating user value. *Acad. Management Rev.* 46(3):534–551.
- Haber B (2019) The digital ephemeral turn: Queer theory, privacy, and the temporality of risk. *Media, Culture & Society* 41(8): 1069–1087.
- Hair JF, Hult GTM, Ringle CM, Sarstedt M (2022) *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 3rd ed. (Sage, Thousand Oaks, CA).
- Hall JA, Park N, Song H, Cody MJ (2010) Strategic misrepresentation in online dating: The effects of gender, self-monitoring, and personality traits. *J. Soc. Personality Relations* 27(1):117–135.
- Hallam L, Walrave W, De Backer CJ (2018) Information disclosure, trust and health risks in online dating. Walrave W, Van Ouystsel J, Ponnet K, Temple JR, eds. *Sexting: Motives and Risk in Online Sexual Self-Presentation* (Palgrave, Nottingham, UK), 19–38.
- Hayes AF (2017) *Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach* (Guilford Publications, New York).
- Heurix J, Zimmermann P, Neubauer T, Fenz S (2015) A taxonomy for privacy enhancing technologies. *Comput. Security* 53:1–17.
- Hitsch GJ, Hortaçsu A, Ariely D (2010a) Matching and sorting in online dating. *Amer. Econom. Rev.* 100(1):130–163.
- Hitsch GJ, Hortaçsu A, Ariely D (2010b) What makes you click? Mate preferences in online dating. *Quant. Marketing Econom.* 8(4):393–427.
- Hofstetter R, Rüppell R, John LK (2017) Temporary sharing prompts unrestrained disclosures that leave lasting negative impressions. *Proc. Natl. Acad. Sci. USA* 114(45):11902–11907.
- Huang N, Burtsch G, He Y, Hong Y (2022) Managing congestion in a matching market via demand information disclosure. *Inform. Systems Res.* 33(4):1119–1516.
- Hui KL, Teo HH, Lee SYT (2007) The value of privacy assurance: An exploratory field experiment. *Management Inform. Systems Quart.* 31(1):19–33.
- Ichihashi S (2021) The economics of data externalities. *J. Econom. Theory* 196:105316.
- Jia T, Spivey RF, Szymanski B, Korniss G (2015) An analysis of the matching hypothesis in networks. *PLoS One* 10(6):e0129804.
- Jiang Z, Heng CS, Choi BC (2013) Research note—Privacy concerns and privacy-protective behavior in synchronous online social interactions. *Inform. Systems Res.* 24(3):579–595.
- John LK, Barasz K, Norton MI (2016) Hiding personal information reveals the worst. *Proc. Natl. Acad. Sci. USA* 113(4):954–959.

- Joinson A (1998) Causes and implications of disinhibited behavior on the Internet. Gackenbach J, ed. *Psychology and the Internet: Intrapersonal, Inter-personal, and Transpersonal Implications* (Academic Press, San Diego), 43–60.
- Jung J, Bapna R, Ramaprasad J, Umyarov A (2019) Love unshackled: Identifying the effect of mobile app adoption in online dating. *Management Inform. Systems Quart.* 43:47–72.
- Jung J, Lim H, Lee D, Kim C (2022) The secret to finding a match: A field experiment on choice capacity design in an online dating platform. *Inform. Systems Res.* 33(4):1248–1263.
- Keith MJ, Maynes C, Lowry PB, Babb J (2014) Privacy fatigue: The effect of privacy control complexity on consumer electronic information disclosure. *Proc. Internat. Conf. on Inform. Systems*, 14–17.
- Kummer M, Schulte P (2019) When private information settles the bill: Money and privacy in Google's market for smartphone applications. *Management Sci.* 65(8):3470–3494.
- Lien CH, Cao Y, Zhou X (2017) Service quality, satisfaction, stickiness, and usage intentions: An exploratory evaluation in the context of WeChat services. *Comput. Human Behav.* 68:403–410.
- Lin T (2022) Valuing intrinsic and instrumental preferences for privacy. *Marketing Sci.* 41(4):235–253.
- Lowry PB, Cao J, Everard A (2011) Privacy concerns vs. desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *J. Management Inform. Systems* 27(4):163–200.
- Lu Y, Tan B, Hui KL (2004) Inducing customers to disclose personal information to Internet businesses with social adjustment benefits. *Proc. 24th Internat. Conf. on Inform. Systems* (ACM, New York).
- Lutz C, Ranzini G (2017) Where dating meets data: Investigating social and institutional privacy concerns on Tinder. *Soc. Media Soc.* 3(1):1–12.
- Mehta S, Dawande M, Janakiraman G, Mookerjee V (2021) How to sell a data set? Pricing policies for data monetization. *Inform. Systems Res.* 32(4):1281–1297.
- Obada-Obieh B, Somayaji A (2017) Can I believe you? Establishing trust in computer mediated introductions. *Proc. New Security Paradigms Workshop*, 94–106.
- Peer E, Acquisti A (2016) The impact of reversibility on the decision to disclose personal information. *J. Consumer Marketing* 33(6):428–436.
- Petronio S (1991) Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Comm. Theory* 1(4):311–335.
- Petronio S (2002) *Boundaries of Privacy* (State University of New York Press, New York).
- Phua J, Jin SV, Kim JJ (2017) Uses and gratifications of social networking sites for bridging and bonding social capital: A comparison of Facebook, Twitter, Instagram, and Snapchat. *Comput. Human Behav.* 72:115–122.
- Piwek L, Joinson A (2016) "What do they Snapchat about?" Patterns of use in time-limited instant messaging service. *Comput. Human Behav.* 54(1):358–367.
- Poltash NA (2012) Snapchat and sexting: A snapshot of baring your bare essentials. *Richmond J. Law & Tech.* 19:1.
- Rifon NJ, LaRose R, Choi SM (2005) Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. *J. Consumer Affairs* 39(2):339–362.
- Rosenfeld MJ (2017) Marriage, choice, and couplehood in the age of the Internet. *Sociol. Sci.* 4(9):490–510.
- Rosenfeld MJ, Thomas RJ, Hausen S (2019) Disintermediating your friends: How online dating in the United States displaces other ways of meeting. *Proc. Natl. Acad. Sci. USA* 116(36):17753–17758.
- Roth AE (2015) *Who Gets What and Why: The New Economics of Matchmaking and Market Design* (Houghton Mifflin Harcourt, Boston).
- Samat S, Acquisti A (2017) Format vs. content: the impact of risk and presentation on disclosure decisions. *Thirteenth Symposium on Usable Privacy and Security (SOUPs 2017)* (ACM, New York), 377–384.
- Saunders JF, Eaton AA (2018) Snaps, selfies, and shares: How three popular social media platforms contribute to the sociocultural model of disordered eating among young women. *Cyberpsych. Behav. Soc. Networks* 21(6):343–354.
- Sedgewick JR, Flath ME, Elias LJ (2017) Presenting your best self (ie): The influence of gender on vertical orientation of selfies on Tinder. *Frontiers Psych.* 8:604.
- Shi L, Huang P (2019) Pragmatic men, romantic women? Performance feedback design on two-sided matching platforms. *Proc. 40th Internat. Conf. on Inform. Systems* (Association for Information Systems, Atlanta).
- Shi L, Viswanathan S (2023) Optional verification and signaling in online matching markets: Evidence from a randomized field experiment. *Inform. Systems Res.* 34(4):1321–1814.
- Statista (2020) Online dating worldwide. Retrieved February 28, 2024, <https://www.statista.com/outlook/372/100/online-dating/worldwide>.
- Steed R, Liu T, Wu ZS, Acquisti A (2022) Policy impacts of statistical uncertainty and privacy. *Science* 377(6609):928–931.
- Suler J (2004) The online disinhibition effect. *Cyberpsych. Behav.* 7(3):321–326.
- Tavani HT, Moor JH (2001) Privacy protection, control of information, and privacy-enhancing technologies. *ACM Sigcas Computers Soc.* 31(1):6–11.
- Taylor LS, Fiore AT, Mendelsohn GA, Cheshire C (2011) "Out of my league": A real-world test of the matching hypothesis. *Personality Soc. Psych. Bull.* 37(7):942–954.
- Teutsch D, Masur PK, Trepte S (2018) Privacy in mediated and non-mediated interpersonal communication: How subjective concepts and situational perceptions influence behaviors. *Soc. Media Soc.* 4(2):2056305118767134.
- Tsai JY, Egelman S, Cranor L, Acquisti A (2011) The effect of online privacy information on purchasing behavior: An experimental study. *Inform. Systems Res.* 22(2):254–268.
- Tucker CE (2014) Social networks, personalized advertising, and privacy controls. *J. Marketing Res.* 51(5):546–562.
- Utz S, Muscanell N, Khalid C (2015) Snapchat elicits more jealousy than Facebook: A comparison of Snapchat and Facebook use. *Cyberpsych. Behav. Soc. Networks* 18(3):141–146.
- Vaterlaus JM, Barnett K, Roche C, Young JA (2016) "Snapchat is more personal": An exploratory study on Snapchat behaviors and young adult interpersonal relationships. *Comput. Human Behav.* 62:594–601.
- Waddell TF (2016) The allure of privacy or the desire for self-expression? Identifying users' gratifications for ephemeral, photograph-based communication. *Cyberpsych. Behav. Soc. Networks* 19(7):441–445.
- Wakefield LT, Wakefield RL (2018) Anxiety and ephemeral social media use in negative eWOM creation. *J. Interactive Marketing* 41:44–59.
- Wang Y, Norcie G, Komanduri S, Acquisti A, Leon PG, Cranor LF (2011) "I regretted the minute I pressed share" a qualitative study of regrets on Facebook. *Proc. 7th Sympos. on Usable Privacy and Security* (Association for Computing Machinery, New York), 1–16.
- Whyte S, Chan HF, Torgler B (2018) Do men and women know what they want? Sex differences in online daters' educational preferences. *Psych. Sci.* 29(8):1370–1375.
- Xu L, Xiang J, Yuan X (2018) Transferring rich deep features for facial beauty prediction. Preprint, submitted March 20, <https://arxiv.org/abs/1803.07253>.
- Xu B, Chang P, Welker CL, Bazarova NN, Cosley D (2016) Automatic archiving vs. default deletion: What snapchat tells us about ephemerality in design. *Proc. ACM Conf. Computer Supported Cooperative Work and Social Comput.* (ACM, New York), 1662–1675.
- Yu M, Riddle K (2022) An experimental test of the effects of digital content permanency on perceived anonymity and indirect effects on cyber bullying intentions. *Soc. Media Soc.* 8(1):20563051221087255.

- Yu Y, Animesh A, Ramaprasad J, Pinsonneault A (2018) Does premium subscription pay off? Evidence from online dating platform. *Proc. 39th Internat. Conf. on Inform. Systems*.
- Zhang Y, Li B, Luo X, Wang X (2019) Personalized mobile targeting with user engagement stages: Combining a structural hidden markov model and field experiment. *Inform. Systems Res.* 30(3): 787–804.
- Zhang NA, Wang CA, Karahanna E, Xu Y (2022a) Peer privacy concerns: Conceptualization and measurement. *Management Inform. Systems Quart.* 46(1):491–530.
- Zhang Y, Ran X, Luo C, Gao Y, Zhao Y, Shuai Q (2022b) “Only visible for three days”: Mining microblogs to understand reasons for using the Time Limit setting on WeChat Moments. *Comput. Human Behav.* 134:107316.