# Designing Opportunistic Social Matching Systems for Women's Safety During Face-to-Face Social Encounters

Caroline Bull
Oakland University
carolinebull@oakland.edu

Hanan Aljasim
Oakland University
hkaljasi@oakland.edu

Douglas Zytko
Oakland University
zytko@oakland.edu

## ABSTRACT

This paper presents emerging findings from a participatory design study with women about how future designs of opportunistic social matching systems can foreground user safety. The study is motivated by a relative lack of focus on user safety in social matching systems (Tinder, Bumble, etc.) in light of advances to user discovery mechanisms that enable increasingly rapid face-to-face encounters. Findings highlight ways that social matching systems could support users' safety after they have left home to pursue a social opportunity in the physical world. Co-designers envisioned a social matching system acting as a "guardian" that genuinely cares for, and monitors, the user's safety even if it cannot flawlessly mitigate harm. Rather than respond only after a definitive harm has occurred, co-designers expected the system to intervene earlier, during ambiguously unsafe or uncomfortable situations. The paper considers directions for future work in response to users' expectations for how social matching systems should coordinate with trusted contacts to intervene in unsafe situations.

## CCS CONCEPTS

• **Social and professional topics** → User characteristics; Gender; • **Human-centered computing** → Collaborative and social computing; Empirical studies in collaborative and social computing.

## KEYWORDS

social matching, opportunistic social matching, women, gender, sexual violence, risk, harm, participatory design, online dating

**ACM Reference Format:**
Caroline Bull, Hanan Aljasim, and Douglas Zytko. 2021. Designing Opportunistic Social Matching Systems for Women's Safety During Face-to-Face Social Encounters. In *Companion Publication of the 2021 Conference on Computer Supported Cooperative Work and Social Computing (CSCW '21 Companion), October 23–27, 2021, Virtual Event, USA.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3462204.3481751

## 1 INTRODUCTION

HCI research has pursued a vision of opportunistic social matching for decades [9, 18]. This entails a multi-purpose social matching system leveraging context awareness to recommend users to relevant, ephemeral social opportunities in the physical world when they can immediately act on them [10, 11]. The opportunities could be individual people with matching interests, group-based activities, or organized events [23]. While the vision of opportunistic social matching is not yet fully realized, the omnipresence of mobile phones—and the wealth of contextual data they collect—is inching us closer. For example, mobile matching apps like Grindr support near instantaneous face-to-face meetings between strangers [2, 8], and Tinder and Bumble are expanding beyond single purposes like dating to support other social endeavors like friendship and employment [4, 7, 19, 20].

The consequences of these user discovery advancements on user *safety* have been relatively overlooked, however. In light of mounting evidence involving mobile social matching system-facilitated harm, such as sexual violence and harassment [1, 3, 5, 6, 12, 13, 15], it is imperative that progress towards the opportunistic social matching vision begin to take user safety more seriously. This is particularly urgent given the stark gender imbalance in such harms—victims of matching app-facilitated sexual violence, for example, are overwhelmingly women [14, 16, 22].

The state of safety-oriented features in social matching systems is severely lacking. While popular social matching apps have increased their focus on safety [21] such features are primarily reactive, requiring users to first be harmed before the feature can be used. Examples include user blocking, user reporting, and a "panic button" that can alert authorities after one has been harmed. Furthermore, such features put the responsibility on would-be victims to respond to harm experienced. Social matching systems seldom play an active role in maintaining a state of safety for users and, more generally, designs give little indication of prioritizing user safety to the same level as user discovery.

In this paper we present emerging findings from a participatory design study with women about safety-conscious directions for opportunistic social matching system design. The study is driven by the following research questions:

***RQ1.*** How do women conceptualize a state of safety during opportunistic social matching system-use?

**RQ2.** How could opportunistic social matching systems be designed to maintain or achieve this state of safety?

## 2 METHOD

To explore our research questions, we are conducting a participatory design study with women to produce safety-conscious designs for tomorrow's opportunistic social matching apps. Participatory design groups have consisted of 4-8 women, with each group attending four 1-hour video chat sessions over Zoom. Four researchers were present in every session. A total of 22 women have attended

*CSCW '21 Companion, October 23–27, 2021, Virtual Event, USA*

ACM ISBN 978-1-4503-8479-7/21/10…$15.00
https://doi.org/10.1145/3462204.3481751

across three groups and they were each compensated $40 for participation. Their ages ranged from 18 to 30; 13 identified as White, 3 as Black, 4 as Asian, and 1 as Middle Eastern. One did not disclose their ethnicity. All participants have been university students due to early recruitment methods leveraging student email lists and direct requests to professors to promote the study in class. Students responded to a screening survey to confirm eligibility to the study. Selected candidates were then emailed a consent form which informed them of session details. Participants represented a variety of majors and departments including Mathematics, Psychology, Communication, and Bioengineering.

Four recurrent participatory design sessions per group were selected to build trust and camaraderie amongst co-designers, minimize fatigue, and increase collaboration in the online sessions. The first session focused on introducing participants to the concept of opportunistic social matching and discussing safety concerns that should be foregrounded in design. The second session involved prompts to design opportunistic social matching interfaces to inform women's decisions to pursue a safe social opportunity. The third session involved reflection of how women would want to control the system's AI pursuant to safety. The final session focused on designs to manage safety once users have ventured off the app to attend a social opportunity. Through all sessions storyboard-based scenarios preceded design activities. Groups were divided into breakout rooms where they discussed and produced sketches through pen-and-paper or online collaborative drawing tools. One researcher remained present in each room. After each design activity, results were shared in the main Zoom area. All design sessions were audio recorded and transcribed. A team of four researchers analyzed the transcripts and visual artifacts with an open coding process inspired by Strauss and Corbin [17]. Researchers applied line-by-line coding in Dedoose, then organized quotes and visual output via Miro to find emergent themes.

# 3 FINDINGS

Our open coding has produced various emerging themes around the roles that opportunistic social matching systems can play pursuant to user safety, which go beyond mere facilitation of user discovery. The theme we present in this paper is the role of *guardian*, which we define conceptually as the social matching app monitoring or observing a user's safety status after they have ventured off the app to pursue a social opportunity in the physical world.

Contrary to concerns of data privacy that typically accompany user tracking on mobile apps, participants expressed willingness to give ample personal data to an opportunistic social matching app for the purpose of being *monitored* when traveling to and engaging in a social opportunity. As one participant explained, they "*felt safer having themselves tracked*" by the system. This offering of personal data was intended to help the social matching system recognize user discomfort or compromised safety status and, ultimately, take responsibility for the user's safety once they have ventured off the app and into the physical world. Interestingly, this responsibility did not require that the system excel at preventing harm. Participants primarily imagined the application *"keeping an eye out"* for users, much in the same way that a parent may recurrently check in with their child who has ventured outside of the home: a practice that may do more for the parent's piece of mind than the child's safety. Keeping with the analogy, some co-designers actually suggested the idea of the app doing a routine *"check-in"* to ask about their safety status, therefore reminding the user of the app's interest in their wellbeing. Participants valued the notion of the app *caring* about their safety to the same extent that it cares about recommending relevant social opportunities.

## 3.1 What Does the Guardian Do with Data from User Tracking?

Co-designers produced various concepts for when and how an opportunistic social matching app should act on the data it collects about users during face-to-face social encounters. These concepts fall into two categories: 1) coordinating *"real people"* support and 2) verifying information about the social encounter.

**Coordinating *"real people"* support:** In addition to the app monitoring a user's safety status, co-designers also envisioned the app serving as a bridge to involving "*real people*"—trusted contacts, friends, or family members—in leveraging app-collected data to monitor the user. Design ideas ranged from predesignating contacts that could voluntarily monitor the user's status at any time once they have left home to pursue a social opportunity, to contacts being alerted in response to particular situations deemed threatening to the user's safety status. Regarding the later, this would involve the application "*automatically [. . .] sending out [for] help*" when it has sensed, or directly been told by the user, that help is needed. This *"help"* would not necessarily require a user to have already been harmed (which is how today's "panic buttons" typically work). Co-designers imagined the bar for alerting trusted contacts to be much lower, such as situations that *"feel unsafe"* or uncomfortable. Alerting contacts, in these cases, is more preemptive than reactive—a signal that assistance may soon be needed to help a user leave a situation early or escort them home.

**Verifying information:** Co-designers envisioned opportunistic social matching apps collecting ample information not just about them, but the social opportunities they would be traveling to and the other users involved in those opportunities. This information would enable users to "*see [..] what the area [meeting place] is*" and confirm that people discovered at the meeting place are "*who they say they are.*"

Below we discuss proposed designs in more detail for coordinating support and verifying information by dividing them into three key stages once the user has ventured away from their home to pursue a social opportunity: 1) traveling to the social opportunity, 2) attending the social opportunity, and 3) returning home from the social opportunity.

## 3.2 The Guardian's Role When a User is Traveling to a Social Opportunity

Concerns commonly brought up by participants when imagining travel to a social opportunity pertained to verifying the legitimacy and safety of the location prior to arrival. A fear frequently broached by co-designers was the possibility of users posting inauthentic social gatherings for the purpose of luring women to unsafe areas. Several participants suggested in their designs that the social matching app could collect and provide pictures of the social opportunity

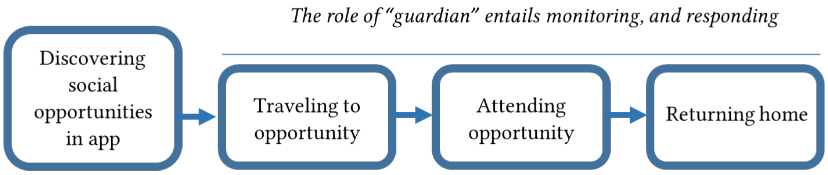
The role of "guardian" entails monitoring, and responding
Discovering social opportunities in app
Traveling to opportunity
Attending opportunity
Returning home

**Figure 1: The social matching app's role of "guardian" does not begin until after the user has left home.**

location for personal inspection. As one participant explained, "I guess one of the most important things to me is just that you can see the area, [you can see] what the area is, related to the activity. I think that would confirm for me that the person is not lying, [and] the area is safe looking."

Some participants elaborated on picture content with the notion of image verification, such as a *"stamp"* that the app could apply to an image to confirm that it accurately depicts the current state of a meeting location. One participant described her design ideas with a scenario in which a social opportunity host sends a picture of the location interior to potential attendees: *"If I saw the image of the cafe, but [...] maybe they took an image of, like, some weird part of the cafe I wouldn't really know. But if the stamp of the image said [...] it was taken at this cafe, then you could be like, okay, well that means it double confirms that the person is in the cafe, and I would feel better."* Relatedly, participants also imagined that the app would "*show you the way to the event"* with GPS-based directions that avoid areas with known safety issues.

Another important design idea that several women supported, pertinent to the category of coordinating support, was a "friends and family on standby" system. Setting up the system would entail the user inputting trusted contacts into the app prior to venturing off to a social opportunity. These contacts would be notified of the user's plan to attend a particular social opportunity and continuously updated on the user's location and safety status. One participant explained the feature in this way: *"I could put in my sister [her contact information] [...] then when I go to an event my sister would receive a notification of 'name' going to 'place' at 10 o'clock and the location."*

## 3.3 The Guardian's Role When a User is Attending a Social Opportunity

Once users arrive at a social opportunity safely, some co-designers envisioned the social matching app prompting the user to confirm the location corresponded with the information they received before arriving. This would serve to reinforce the validity of picture content sent to other users interested in, or still traveling to, the social opportunity. In the words of one participant: *"I was thinking of a verification that pops up after, say, 5 or 10 minutes after you get to the event asking, 'Hey, is this event real? [Does] this event seems alright?' So that it helps not only the system now but also the system can let others know that seems alright by other people."* Co-designers consistently requested that the social matching app continue to track their status once they arrived at a social opportunity safely. Examples of such tracking mostly pertained to the user's location, which co-designers considered a vital piece of information to convey to their "friends and family standby" system. If they ever needed to alert one of their trusted contact that intervention is needed, real time location information could be provided so one's contacts could find them quickly.

Considering that social opportunities in opportunistic social matching apps may involve multiple people, such as events and group activities, participants considered ways that the app could verify the identities of different people discovered at a group-based social opportunity. One group of co-designers sketched a solution to this that involved mutual scanning of QR codes: "*it's [. . .] something to confirm your identity, I was thinking like QR codes, so you both have to pull up the app that displays a QR code and you can both scan each other's and it'll tell you if the person is the right person [a host or attendee of the social opportunity] or not."*

Another suggested safety feature was an *"I feel unsafe button"* which gives users the power to notify the app and, by extension, their friends and family in "standby" mode if they need to leave with outside assistance. The choice of words *"I feel unsafe"* is deliberate to emphasize that women should not have to wait until harm has already occurred to seek assistance. Co-designers elaborated on the *"I feel unsafe button"* by considering data that the app could collect to predict unsafe situations. Some participants recommended biometric data from wearable devices to assist with this: "*If you have a Fitbit that can read your heart rate or your temperature, anything. [...] Just having [a notification] pop up somehow like "do you feel unsafe", "do you need help" and then you would just press the button that would pop up."*

## 3.4 The Guardian's Role When a User is Returning Home from a Social Opportunity

Participants envisioned that opportunistic social matching apps would continue to monitor their safety status until their return home from a social opportunity. There were two priority concerns when the user leaves a social opportunity: stalking and abduction. The proposed solution was to utilize GPS tracking to monitor relative location of attendees (determined by previous QR code check ins) and notify users if any attendees remain in unusually close proximity to them while traveling home. One participant expressed the feature in this way: *"So, say you attended an event. And maybe there was somebody there that was a little bit creepy, maybe into you, but [you don't like them]. So you go home, [. . .] you then get a notification that, hey, this person you just met is in your area. [. . .] This is a sort of checking of behavior patterns for your phone."*

Participants also wanted the system to check in with them after the social opportunity ended to confirm their safe return home. To assure that an abductor could not subvert this check-in the app would prompt the user to input a code or *"safe word"* at a designated time. Upon inputting the code, GPS monitoring would cease and all trusted contacts on standby would be notified of their safe return. If the code is not entered, co-designers indicated that the system should send an automated text message to trusted contacts prompting them to confirm the user's safety.

## 4 DISCUSSION AND FUTURE WORK

In this paper we presented early findings from a participatory design study with women about how future designs for opportunistic social matching systems can foreground user safety. The study reveals several possible approaches for involving social matching apps in user safety after users have ventured out of their homes to pursue a social opportunity. This runs in stark contrast to today's social matching app designs, which play little if any role while users are traveling to, and attending, a social opportunity in the physical world.

The findings show that users expect social matching systems to do more than matching and take responsibility for users' safety, even if the system cannot necessarily guarantee safety or mitigate harm. Co-designers were surprisingly willing to provide extensive data to help social matching systems monitor their safety status, including granular real-time location, biometric data, and contact information of their friends and family. In addition, they wanted to reduce standards for when the social matching system should intervene in the user's situation. Whereas typical safety features today mostly react to a harm that has already occurred, co-designers imagined social matching systems intervening earlier, when situations feel vaguely unsafe or uncomfortable.

Another function that co-designers envisioned for opportunistic social matching systems was to serve as a bridge to trusted contacts who, rather than only responding to definitive harm, could actively monitor a user's status alongside the app and support the user at any point in their social opportunity journey. A direction for future work is to probe into this app-to-trusted-contact bridge more in depth, to answer questions such as: what information do trusted contacts want to receive and, more generally, how can opportunistic social matching systems support these trusted contacts to rapidly intervene. Future work should also consider how social matching app design may alter the behavior of would-be perpetrators and therefore reduce the onus on would-be victims to ensure safety.

## REFERENCES

[1] Monica Anderson, Emily A. Vogels, and Erica Turner. 2020. The virtues and downsides of online dating. *Pew Research Center report.* Retrieved from https://www.pewresearch.org/internet/2020/02/06/the-virtues-and-downsides-of-online-dating/

[2] Courtney Blackwell, Jeremy Birnholtz, and Charles Abbott. 2014. Seeing and being seen: Co-situation and impression formation using Grindr, a location-aware gay dating app. *New Media Soc.* (2014), 1–20. DOI:https://doi.org/10.1177/1461444814521595

[3] Edmond Pui Hang Choi, Janet Yuen Ha Wong, and Daniel Yee Tak Fong. 2018. An emerging risk factor of sexual abuse: the use of smartphone dating applications. *Sex. Abus.* 30, 4 (2018), 343–366.

[4] Stefanie Duguay, Jean Burgess, and Nicolas Suzor. 2020. Queer women's experiences of patchwork platform governance on Tinder, Instagram, and Vine. *Convergence* 26, 2 (2020), 237–252.

[5] Louisa Gilbert, Aaron L Sarvet, Melanie Wall, Kate Walsh, Leigh Reardon, Patrick Wilson, John Santelli, Shamus Khan, Martie Thompson, Jennifer S Hirsch, and others. 2019. Situational contexts and risk factors associated with incapacitated and nonincapacitated sexual assaults among college women. *J. Women's Heal.* 28, 2 (2019), 185–193.

[6] Rosalie Gillett. 2018. Intimate intrusions online: Studying the normalisation of abuse in dating apps. In *Women's Studies International Forum*, 212–219.

[7] Joey Chiao-Yin Hsiao and Tawanna R Dillahunt. 2017. People-nearby applications: How newcomers move their relationships offline and develop social and cultural capital. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, 26–40.

[8] Christian Licoppe, C.A. Riviere, and J. Morel. 2016. Proximity awareness and the privatization of sexual encounters with strangers The case of Grindr. In *Context Collapse: Re-assembling the Spatial*, Carolyn Marvin, Sun-Ha Hong and Barbie Zelizer (eds.). London, UK: Routledge.

[9] Julia Mayer and Quentin Jones. 2016. Encount'r: Exploring Passive Context-Awareness for Opportunistic Social Matching. In *Proceedings of the 19th ACM Conference on Computer Supported Cooperative Work and Social Computing Companion*, 349–352.

[10] Julia M Mayer, Starr Roxanne Hiltz, Louise Barkhuus, Kaisa Väänänen, and Quentin Jones. 2016. Supporting opportunities for context-aware social matching: An experience sampling study. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 2430–2441.

[11] Julia M Mayer, Starr Roxanne Hiltz, and Quentin Jones. 2015. Making social matching context-aware: Design concepts and open challenges. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 545–554.

[12] Anastasia Powell and Nicola Henry. 2019. Technology-facilitated sexual violence victimization: Results from an online survey of Australian adults. *J. Interpers. Violence* 34, 17 (2019), 3637–3665.

[13] Ronald D. Rogge, Dev Crasta, and Nicole Legate. 2020. Is Tinder–Grindr Use Risky? Distinguishing Venue from Individuals' Behavior as Unique Predictors of Sexual Risk. *Arch. Sex. Behav.* 49, 4 (2020), 1263–1277. DOI:https://doi.org/10.1007/s10508-019-01594-w

[14] Janine Rowse, Caroline Bolt, and Sanjeev Gaya. 2020. Swipe right: the emergence of dating-app facilitated sexual assault. A descriptive retrospective audit of forensic examination caseload in an Australian metropolitan service. *Forensic Sci. Med. Pathol.* (2020), 1–7.

[15] Gilla K. Shapiro, Ovidiu Tatar, Arielle Sutton, William Fisher, Anila Naz, Samara Perez, and Zeev Rosberger. 2017. Correlates of Tinder Use and Risky Sexual Behaviors in Young Adults. *Cyberpsychology, Behav. Soc. Netw.* 20, 12 (December 2017), 727–734. DOI:https://doi.org/10.1089/cyber.2017.0279

[16] Frances Shaw. 2016. "Bitch I said hi": The Bye Felipe campaign and discursive activism in mobile dating apps. *Soc. Media+ Soc.* 2, 4 (2016), 2056305116672889.

[17] Anselm Strauss and Juliet M Corbin. 1990. Basics of Qualitative Research: Grounded Theory Procedures and Techniques. Sage Publications, Inc.

[18] Loren Terveen and David W McDonald. 2005. Social matching: A framework and research agenda. *ACM Trans. Comput. Interact.* 12, 3 (2005), 401–434.

[19] Elisabeth Timmermans and Elien De Caluwé. 2017. Development and Validation of the Tinder Motives Scale (TMS). *Comput. Human Behav.* 70, (2017), 341–350. DOI:https://doi.org/10.1016/j.chb.2017.01.028

[20] Elisabeth Timmermans and Cédric Courtois. 2018. From swiping to casual sex and/or committed relationships: Exploring the experiences of Tinder users. *Inf. Soc.* 34, 2 (2018), 59–70.

[21] Tinder. Tinder Introduces Safety-Focused Updates. *Tinder Blog*. Retrieved May 31, 2020 from https://blog.gotinder.com/tinder-introduces-safety-updates/

[22] UK National Crime Agency. 2016. *Emerging new threat in online dating: Initial trends in internet dating-initiated serious sexual assaults.* National Crime Agency London, England. Retrieved from https://trends.ifla.org/node/425

[23] Douglas Zytko and Dalvin Josias Sejour. 2018. Encounter Opportunity Browsing: A New Approach to Opportunistic Social Matching. In *Companion of the 2018 ACM Conference on Computer Supported Cooperative Work and Social Computing*, 357–360.