Foregrounding Women's Safety in Mobile Social Matching and Dating Apps: A Participatory Design Study

HANAN KHALID ALJASIM, Oakland University, USA
DOUGLAS ZYTKO, Oakland University, USA

The design of social matching and dating apps has changed continually through the years, marked notably by a shift to mobile devices, and yet user safety has not historically been a driver of design despite mounting evidence of sexual and other harms. This paper presents a participatory design study with women—a demographic at disproportionate risk of harm through app-use—about how mobile social matching apps could be designed to foreground their safety. Findings indicate that participants want social matching apps to augment women's abilities for self-protection, reflected in three new app roles: 1) the cloaking device, through which the social matching app helps women dynamically manage visibility to geographically nearby users, 2) the informant, through which the app helps women predict risk of harm associated with a recommended social opportunity, and 3) the guardian, through which the app monitors a user's safety during face-to-face meetings and augments their response to risk.

CCS Concepts: • **Human-centered computing** → **Participatory design**; • **Social and professional topics** → **Women**.

Additional Key Words and Phrases: online dating, dating apps, social matching, women, feminist HCI, harm, risk, sexual violence, participatory design

ACM Reference Format:
Hanan Khalid Aljasim and Douglas Zytko. 2023. Foregrounding Women's Safety in Mobile Social Matching and Dating Apps: A Participatory Design Study. *Proc. ACM Hum.-Comput. Interact.* 7, GROUP, Article 9 (January 2023), 25 pages. https://doi.org/10.1145/3567559

1 INTRODUCTION

"Designers are not passive bystanders in the production, reproduction, reinforcing, or challenging of cultural values. We actively create artifacts and experiences. We design products with implicit or explicit assumptions about how products will be used and by whom." [23]

Mobile social matching and dating apps have transformed the ways in which we augment our social lives. Once a niche technology, the use of such apps for discovering romance partners, friends, and even employment opportunities has become culturally normalized. But what assumptions, values, and priorities underpin their design?

Progression in social matching app design—from websites accessed on desktop computers to mobile applications—have prioritized expanded awareness of nearby others and increasingly rapid pace towards face-to-face encounters, which we argue to be masculine values through the lens of sexual strategies theory [20]. Users of today's social matching apps can meet a stranger within

Authors' addresses: Hanan Khalid Aljasim, Oakland University, 318 Meadow Brook Rd, Rochester, Michigan, USA, hkaljasi@oakland.edu; Douglas Zytko, Oakland University, 318 Meadow Brook Rd, Rochester, Michigan, USA, zytko@oakland.edu.

2573-0142/2023/1-ART9 $15.00
https://doi.org/10.1145/3567559

minutes (or less) given granular geographic proximity matching (e.g., "this user is 500 feet away"). Motivated by feminist HCI [8] and rejection of universal usability, we challenge the notion that these advancements in social matching app design are universally desired. For evidence of this we turn to the mounting literature indicating that victims of social matching app-facilitated sexual violence and harassment are disproportionately women [1, 3, 22, 41, 42, 73, 76, 81, 93], which often culminates in them leaving the platform. And despite continued critique of social matching app design for safety [32, 74, 114] design innovation has not traditionally foregrounded this concern. While acknowledging that dating apps such as Tinder and Bumble have recently added new AI implementations for detection of online harms such as harassing messages and cyberflashing, safety-oriented features have more commonly been reactive in nature, such as user blocking, reporting, and panic buttons during face-to-face encounters, meaning women must first be harmed in order for such features to be usable.

The experiences of women, and their conceptualizations of safety, urgently need to be foregrounded in social matching app design to produce a more equitable user experience—one that pursues comparable safety outcomes regardless of gender. Given evidence that dating apps are transforming into multi-purpose social matching apps [50, 70, 94, 95], userbases are poised to grow and thus expose new audiences to harm which, if unchecked, can become normalized and pose a barrier to app-use or, worse, have detrimental impacts on women's sense of sexual agency and self-protection. For example, research into Tinder has found women to justify sexual harassment on the platform as normal given its frequency, with some even apologizing to harassers for rejecting their sexual advances [109].

In this paper we present a participatory design study with 22 women in the United States about how multi-purpose social matching apps can be designed pursuant to their vision of safety. The research questions driving the study are:

RQ1. *What are the current or anticipated risks of mobile social matching app-use that should be foregrounded in design?*
RQ2. *How do women conceptualize a state of safety during mobile social matching app-use?*
RQ3. *How could mobile social matching apps be designed to maintain or achieve this state of safety?*

While participants referenced various potential harms that concern them **(RQ1)**, they wanted social matching apps to primarily address the risk of helplessness, or the inability of women to effectively manage risk of harm. They conceptualized safety during social matching app use **(RQ2)** as a reduction in risk of helplessness through improved personal awareness and control over risk of harm associated with strangers they choose to meet face-to-face or may inadvertently encounter in the geographic vicinity. Participants acknowledged that social matching app design could never fully mitigate risk of harm, nor would they expect it to. Their proposed designs **(RQ3)** sought to augment women's abilities to manage risk of harm with three new roles for mobile social matching apps: 1) the cloaking device for managing visibility to nearby others, 2) the informant for crowdsourcing awareness of risk with a potential face-to-face encounter, and 3) the guardian for monitoring a user's safety status during face-to-face meetings and augmenting their response to risk or actualized harm. The paper concludes with a reflection on the potential impacts—both positive and negative—of the proposed designs to inform a future course for safety-conscious design of online-to-offline social encounters.

2 BACKGROUND

In this section we first review HCI research into disparities in technology-use for women and increasing attention that has been given to technology for women's health, including technology

that perpetuates and also seeks to stop violence against women. We build on this literature to motivate design for mitigation of harms perpetuated through social matching and dating app-use, for which women are disproportionately victimized. We then review the extent of harms perpetuated by social matching and dating apps and the historically minimal focus on safety in progressions of their design. The section concludes by making the case for a participatory design approach in light of prior attempts to design for safety in social matching apps that are problematic or dubiously effective.

2.1 Violence Against Women and HCI

Over the past few decades HCI research has consistently highlighted disparities in user experience of technology for women. Some of this research has pursued gender-inclusive design [18, 19] through individual differences in software-use on the basis of gender [9] or disparities in participation of online activities such as peer production on Wikipedia [36]. Spurred by feminist HCI [8] and a more explicit focus on perspectives traditionally marginalized in design, mounting attention has been given to how technology could augment women's health [54]. Examples include technologies for menstruation [7, 98] and design of breast pumps [30].

Another line of research has focused on the role of technology in violence against women, including how computer-mediated communication facilitates harm and how technologies could potentially be designed as solutions. The public health literature has repeatedly confirmed gender disparities in sexual and domestic violence [63, 85, 105], and such disparities are maintained with computer-mediated harms. Research within and beyond HCI consistently positions women as disproportionately affected by including online harassment and abuse [78, 79, 101], intimate partner violence [37, 38], cyberstalking [56], and revenge porn [60]. They are also disproportionately the victims of online-to-offline harms such as use of social media to coerce individuals into sex trafficking [75, 102] and rape facilitated through dating apps [76].

Computer-mediated solutions in the literature for violence against women have been wide ranging and representative of women all around the world including Brazil [68], Korea [107], and South Asia [79] including India [53], Bangladesh [2, 64], and Pakistan [80]. Some of this literature pertains to solutions integrated into social media platforms, such as AI for sexual risk detection and content moderation [75, 90], conversational agents for support-seeking of sexual violence survivors [69], and how social media can be used for post-harm support [5] and reframing of experience [31]. Others have considered mobile and wearable technologies to intervene in gender-based harm that occurs in the physical world [4, 16]. These include mobile applications to support deaf women against domestic violence [68] as well as wearable devices to monitor women's safety [77] and deter rapists through odor emitting capsules and alarms [65]. Additional examples include MehfoozAurat, a mobile app to protect women from lower socio-economic brackets in Pakistan with safe routes and emergency alerts [80], Protibaadi, a wearable device to assist women in Bangladesh to discretely seek help when being sexually harassed [2], and Anshimi, a mobile app to provide women in Korea with safety services through collection of data such as GPS location [107].

Our study builds on this prior work into technology design for women's safety by focusing on harms specifically perpetuated through social matching and dating apps.

2.2 Mobile Social Matching Apps and Perpetuation of Harm Against Women

Mobile social matching apps are systems accessed through mobile devices that recommend people to people [92]. The most popular social matching apps are typically associated with dating [27, 33] as exemplified by Tinder, Bumble, OkCupid, and Grindr. They have three standard components: a profile page for each user that usually includes their pictures and other text content, a mechanism for recommending users to one another, and capabilities for one-to-one interaction.

Mobile dating apps have been linked with various harms and health risks [3] including STI/HIV infection [45, 103, 104], online harassment [6, 24, 82], and stalking [21]. Several studies have also connected dating apps with sexual violence [1, 3, 22, 41, 42, 73, 76, 81, 93]. Studies of sexual violence in Australia found a sizeable portion of overall cases to be attributable to dating apps [73, 76] – in one study all victims were women. Other studies have found that dating app users are more likely to be sexual abused [22] and more likely to report nonconsensual sex than non-users [81]. Research also indicates that the problem is worsening: rates of dating app-facilitated rape in the UK, for example, increased six-fold over a five-year period [1]. In line with general statistics on sexual violence [39, 85], SV facilitated through these apps is a gendered problem with victims predominantly identifying as women.

While safety has taken on a more prominent role in the last couple years for dating app companies, as evidenced by Match Group's Trust and Safety Center, harm mitigation has not historically been a driver of social matching app design despite continued critique [32, 74, 114]. In the following subsections we unpack reasons why mobile social matching apps perpetuate harm and why we need increased focus on safety-conscious design.

2.2.1 Risk of Location-Based Matching Apps. The most notable update to social matching app design in recent years has been to user discovery through the leveraging of geographic proximity on mobile devices, thus enabling increasingly rapid face-to-face meetings. Location is incorporated in two ways. One is real-time proximity awareness in which users discover others who are currently geographically nearby. There are two "visibility mechanisms" [28] applied to real-time proximity awareness: Grindr's approach in which thumbnail pictures of several users are displayed on a grid sorted by nearest proximity [11], and Tinder's approach in which profiles of nearby users are discovered one by one. The other way location has been utilized is post-hoc location overlap [59, 100] as exemplified by the dating app happn, in which users are recommended to each other after they have physically "crossed paths" such as on the way to work or while at a mall.

The literature has elucidated several risks associated with location. Some are data privacy risks [34, 49, 83] including concern over how social matching app companies are utilizing extremely detailed location data [58] (for instance, Grindr was fined for its handling of user data [87]). New social risks are also enabled through location such as stalking - the dating app happn reduced granularity of location data in response to concerns from women [100]. Research into Grindr and other apps for men seeking men have depicted user concerns with loss of control over revealing their sexuality and interest in sex to nearby others [15]. Exposure of one's LGBTQ+ identity can incur abuse and social ostracism [57]; risks that are particularly poignant in culturally marginalized locations such as India [12] and rural areas [46].

Users have three capabilities to manage their location visibility depending on the app. The most common involves toggling the visibility of one's entire profile. This is intended for users wanting to take a break from the app rather than active users who want to manage safety because the feature prevents one's profile from being discovered by anyone, therefore making the matching process unusable. Tinder also has a "passport" feature in which users can change their location in the app to anywhere on earth (but can then only discover users in that manually selected location). Lastly, apps for men seeking men such as Grindr allow users to hide their proximity information from their profile while still being able to discover other users, however researchers have demonstrated how a user's location can still be identified with this setting on [49]. Tinder provides a similar feature for a monthly subscription fee which can put it out of reach for users of lower socioeconomic status [21].

The effectiveness of hide-location features on safety is debatable. Researchers have aired concern that a user's location could still be inferred [49], and one study found no significant impact on

the likelihood of harm when women hide location on their profile [21]. **Ultimately, location data has transformed social matching apps into facilitators of near-instantaneous social encounters, yet the design of location-based features have not sufficiently acknowledged the new risks that they expose users to, particularly those from marginalized groups.**

2.2.2 From Dating Apps to Multi-Purpose Social Matching Apps: Expanded Opportunity for Harm. The omnipresence of mobile phones and associated contextual data capabilities has initiated a gradual evolution in dating apps towards multi-purpose social matching apps that are used for various social opportunities [61]. For example, Tinder and Bumble are expanding beyond their singular dating purpose to support other social connections [32, 50, 94, 95]. Bumble's interface has three separate user discovery modes to find other users for dating, friendship, and employment connections. Tinder has previously experimented with a group-based feature called Tinder Social. Importantly, users are also driving this transition of dating apps towards multi-purpose matching apps. While variations in dating app-use for long-term romance and casual sexual encounters have been well known [13, 14, 25, 106, 111], research [50, 70, 94, 95] indicates that modern use of dating apps is driven by more diverse social motivations. Petrychyn and colleagues discovered that women use dating apps for friendship and developing a sense of community with other women [70]. Hsiao and colleagues [50] found dating apps to be used for more general social capital building. Timmermans found use of Tinder to be motivated by 13 different goals [94]. Recent work has also sounded the alarm on new harms that could be facilitated through expanded social matching app-use. For example, more varied use obfuscates users' reasons for using a social matching app and misunderstandings in intent to meet face-to-face could culminate in sexual harm [113]. **The transition of dating apps into multi-purpose social matching apps should be cause of concern given the current state of harm mitigation on such platforms. As userbases continue to rise [6], and for increasingly diverse purposes, more users are poised to be exposed to online-to-offline harm thus motivating urgent design intervention.**

2.3 The Case for Participatory Design of Mobile Social Matching Apps with Women

Mobile social matching apps have seen relatively little innovation for prevention of interpersonal harm. Existing safety features are traditionally reactive in nature, meaning they require a user to be harmed (and to recognize the behavior as harmful) before corrective action is taken. Examples are blocking, muting, and reporting features that users can employ in response to harmful content they have already received in messages or witnessed on profiles. Panic buttons have also been incorporated into dating app design [96], which are intended for use during face-to-face meetings to alert authorities of an emergency. Other features like hiding proximity information from one's profile [21], as well as Bumble's feature requiring women to send the first message to users they have matched with [74], have been criticized for dubious safety effectiveness.

The history of these minimally effective safety features suggests that women should be involved earlier in design. One approach is usability testing of new safety features, but as Zytko and colleagues have demonstrated [114] the testing of new safety features can incur discomfort and unexpected reactions from women which may be avoidable if women are involved in producing, rather than only reacting to, novel designs.

We advocate for a more proactive participatory approach in which women act as designers themselves to propose new designs that fulfill their visions of safety. Participatory design with marginalized groups has proven valuable for informing immediately implementable systems [88] as well as longer-term design agendas [43]. The most applicable example to our work is Haimson and colleague's participatory design study with trans people [43] to elucidate challenges in need of intervention and to articulate conceptual solutions, some of which may not be

immediately practical but can serve as a long-term guiding force for future technologies. We employ a similar approach with women in the context of safety in mobile social matching apps. There are other examples of participatory design being an effective method for involving women in design of technologies to augment their lives. The early stages of developing a menopause app leveraged participatory design with pre-menopause and menopause women to elicit design requirements [97]. Another example involved inclusion of incarcerated women in the design of VR-based reentry training for prisoners [91].

3 METHOD

We conducted a participatory design study with woman-identifying stakeholders in the United States (n=22) to produce new conceptual designs for multi-purpose social matching apps that foreground their safety. Participatory design [66] is a method in which anticipated users and other stakeholders of a technology are incorporated into the design process as designers themselves to ensure that their experiences and perspectives are considered. The study was approved by our university's institutional review board (IRB).

3.1 Participant Recruitment

A two-step process was used to recruit woman-identifying participants. First, advertisements for the study were disseminated to students at a university in the Midwest region of the United States through a student mailing list and through promotion by professors to their classes in a variety of departments ranging from Computer Science, Psychology, Engineering, Nursing, and Communication. We opted for this approach first due to convenience, but also to align with typical demographics of social matching apps users. According to the latest Pew research on dating apps (a subset of matching apps), users are predominantly aged 18-29 and college educated [6]. We subsequently employed snowball sampling.

The recruitment advertisement clarified the purpose of the study as collaboratively designing social matching and dating apps for women's safety. Inclusion criteria specified that participants should identify as women, have previously used a social matching app or would consider using one in the future, and have prior experience with harm or threats to safety through social matching app-use and/or through other dating contexts. There were two reasons we did not make prior social matching app-use a requirement for participation. One, we did not want to exclude women who have not used such apps *because* of their current safety implications and two, we wanted to garner participation of prospective users who may be drawn to social matching app-use in the future for diverse social goals if safety is improved.

A total of 22 women participated in the study. Ages ranged from 18 to 30 and they identified as White (13), Asian (4), Black (3), and Middle Eastern (1). One participant did not disclose their ethnicity. All participants had some college education experience in a range of majors: six in Psychology, five in Information Technology, four in Computer Science, two in Communication, one in Computer Engineering, one in Bioengineering, one in Mathematics, and one in Biomedical Science. Fifteen participants had previously used a social matching app, and 7 had not at the time of study. Social matching apps that had been used by the 15 participants with prior experience included Tinder (11), Bumble (7), Hinge (2), OkCupid (1), and Hot or Not (1); some used more than one. Purposes for past or potential future use of social matching apps by all participants included romance (20), friendship (10), and social activity partners (15). See Table 1 for demographic information per participant.

The 22 participants were split into three groups based on prescheduled meeting times that participants selected from in the recruitment survey. Each group attended four 1-hour participatory design sessions over Zoom. The participatory design activities were spread across sessions to

Table 1. Demographic details of interview participants

P#	Group #	Matching apps used	Frequency of app-use	Ethnicity	Age
1	1	n/a	n/a	Asian	25
2	1	Tinder, Bumble	Few times a week	White	22
3	1	Unnamed/other	One time only	White	22
4	1	Bumble, OkCupid, Hinge	Once a day	Black	26
5	1	Tinder, Bumble	Once a day	Undisclosed	24
6	1	Tinder	Once a month	Black	20
7	1	Tinder	Once a month	Asian	30
8	1	n/a	n/a	White	22
9	2	Tinder, Bumble	Once a week	White	21
10	2	Unnamed/other	Once a week	Asian	18
11	2	Tinder	Few times a week	Black	21
12	2	Tinder	Once a week	White	21
13	2	n/a	n/a	White	21
14	2	n/a	n/a	White	19
15	2	Tinder, Bumble	Few times a week	White	21
16	2	Tinder, Hot or Not	Once a week	White, Asian	20
17	2	Bumble, Hinge	Once a week	White	19
18	2	Tinder	Few times a week	White	21
19	3	n/a	n/a	White	24
20	3	n/a	n/a	Asian	20
21	3	Tinder, Bumble	Once a week	White	19
22	3	n/a	n/a	Middle Eastern	18

decrease participant fatigue and to gradually build trust and camaraderie amongst participants. The first group consisted of 8 participants and all four of their Zoom sessions were conducted in one week. The second group consisted of 10 participants with one Zoom session occurring each week over a 4-week period. The third group consisted of 4 participants and all four Zoom sessions were conducted in one week. Participants were each compensated with a $40 virtual gift card at the completion of the fourth session.

3.2 Precautions for Participant Care and Safety

In anticipation of some participants having previously experienced harm through social matching apps we consulted with a certified Sexual Assault Nurse Examiner who has practiced with a community-based agency for more than nine years as well as a Psychology researcher with experience studying sexual violence to inform best practices for discussing past experiences of harm. We also consulted applicable staff to understand our responsibilities as mandatory reporters of Title IX violations that may be disclosed during the study given that our sample was predominantly university students. It was determined that experiences of sexual harm disclosed by participants were exempt from mandatory reporting.

The participatory design sessions were led by a student researcher identifying as a woman and ethnic minority, which we considered important for developing common ground and comfort with participants. Two male-identifying student researchers were also present in Zoom sessions for activity support (e.g., handling Powerpoint slides, technical difficulties). Both had completed certifications on ethical conduct of research and were trained on best practices for sexual violence research. In accordance with those best practices, participants were given the option to ask the

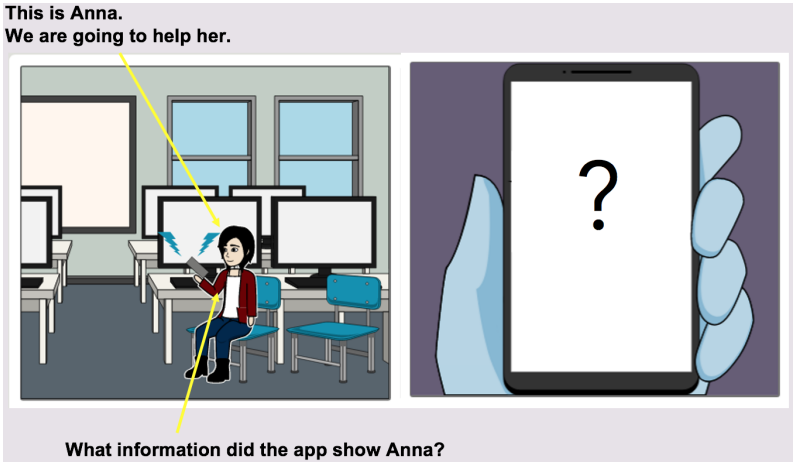

Fig. 1. An example scenario from design session 2 in which our persona "Anna" interacts with a social matching app to discover social opportunities and determine whom to meet face-to-face.

male-identifying researchers to leave the call at any point if they felt uncomfortable (none exercised this option; some actually requested their presence in breakout rooms for technical assistance with sketching). To maintain participant privacy they were asked to keep cameras off and adopt fake names.

3.3 Data Collection and Analysis

The four participatory design sessions revolved around a collection of storyboard scenarios depicting a woman persona using an unnamed social matching app to pursue various social opportunities that ranged from dating, friendship, and partners for specific social activities. The scenarios were informed by prior research about why and how social matching apps are used [50, 70, 89, 95, 109, 110], and were honed through pilot assessment with woman-identifying colleagues and acquaintances (see Figure 1 for an example). Each scenario motivated open discussion about the situation, followed by a design exercise to create a solution that would maintain the persona's safety. Storyboard scenarios have played important roles in participatory design studies, particularly for technologies impacting users' health [10, 67, 72, 88, 97, 99]. They leverage context to elicit specific problems and considerations that can motivate design [10, 99] and enable participants to articulate how and where their envisioned technologies are used [88, 97]. We found these advantages particularly valuable given the mobile and contextual aspects of mobile social matching app-use. Most importantly, we opted for scenarios to ground our participants' designs in relatable contexts of use without requiring them to disclose personal experiences with harm. By designing for a woman persona instead of directly for themselves, participants could use their personal experiences to motivate design but without having to disclose those experiences to researchers and other participants if not comfortable.

The first design session began with a primer on social matching app design including popular apps, common interface design choices, and current features for safety. The primer also included research findings pertaining to their increasing usage and design for non-dating reasons. Participants were welcomed to interject or spark dialogue about primer content. They were then introduced to storyboard scenarios intended to explore RQ1 and 2, which depicted different locations in which a persona user "Anna" uses a social matching app to discover strangers for face-to-face meetings.

These motivated open discussion about risks of harm that the participants anticipated Anna wanting to mitigate, along with conceptualizations of what a "state of safety" means in regards to social matching app-use. Sessions 2-4 sought to explore RQ3, with each session having a different design theme and associated scenarios with Anna. The theme of session 2 was safety-conscious designs of social matching apps while Anna is browsing social opportunities discovered in the app and deciding whom to meet face-to-face. The theme of session 3 was repurposing AI in social matching apps for safety rather than just user discovery. This included primers on conceptual definitions of AI and related terminology like machine learning, as well as examples of how AI is currently applied in dating apps. Session 4's theme was maintaining safety after Anna has decided to meet a person or group of people discovered in the social matching app. After reviewing a respective storyboard participants engaged in sketching activities individually or in pairs to produce design concepts, followed by presentation of their produced sketches to the broader group for open reflection and iteration.

All Zoom sessions were video-audio recorded and transcribed. A three-person team led by a woman-identifying researcher followed a semantic approach to reflexive thematic analysis [17] in which Dedoose was used to collectively code and re-code the transcripts through a series of synchronous meetings. A Miro board was used in subsequent rounds of meetings to organize and re-organize all quotes and visual artifacts into categories and themes. The first round of Miro board-based organization revolved around placing proposed social matching app designs into categories based on where said features would be used in the life cycle of app use (e.g., while browsing social opportunities, while meeting someone face-to-face, while returning home). The second and third rounds incorporated themes around anticipated risk and conceptualizations of safety and how they relate to proposed designs, which led in final rounds to a re-organization of proposed designs around three new "roles" of social matching apps pursuant to conceptualizations of safety.

4 LIMITATIONS

This study has some limitations that should be acknowledged. Participants all had some college experience and resided in the Midwest United States. We need to acknowledge the relative privilege of this population, which may impact how they perceive safety, and the likelihood that their experiences and ideas will not reflect those of other non-US and non-college educated populations. Furthermore, because interface designs were abstract and early stage, the potential adverse impacts of participants' proposed designs could not be fully considered. The needs and anticipated use of the proposed designs by stakeholders may change if their ideas are adapted into app design.

5 FINDINGS

RQ1. Risks to be foregrounded in design: Participants elucidated several harms that they had either previously experienced as social matching app users or were concerned about experiencing in the future. Harms mentioned by participants across sessions included kidnapping and sex trafficking, sexual assault, stalking, financial scams, and physical harm. These various harms were subsumed by an overarching *risk of helplessness*, or loss of control over which harms women are susceptible to as social matching app users.

RQ2. Conceptualizing a state of safety: A state of safety during social matching app-use was conceptualized not as the complete absence of risk, but rather as personal awareness and management over risk of harm (the converse of risk of helpless). Participants acknowledged that there will always be some risk to meeting new people, and they did not expect social matching apps to be flawless mitigators of harm. On the contrary, many were skeptical of social matching apps

being able to *"protect"* them, and they resisted notions of a social matching app supplanting their own capabilities for self-protection because it would not address the overall risk of helplessness.

In P12's words: *"There is risk to any [social] activity. And if you're going to be with an individual, you need to trust the individual. And I personally wouldn't anticipate that any software that I'm using to interact with an individual is going to protect me from anything like, I wouldn't anticipate that the app would do any sort of protection, and I wouldn't trust it to do any sort of protection. So you think that's all [you need to do] to protect yourself, you will not. I guess, as an individual, I wouldn't expect there to be any system in place to protect a user from another individual."*

RQ3. Designing social matching apps for safety: Proposed designs sought to reduce risk of helpless through augmentation of women's abilities to protect themselves. Participants often personified a future social matching app as a partner in risk management, working in tandem with the user to maintain their agency over risk exposure, to enrich their existing strategies for self-protection, and to amplify their awareness of risk. In order to augment user awareness and control of risk, participants envisioned social matching apps being used beyond discovery and online interaction with prospective meeting partners. They expected the app to offer utility for risk management while also traveling to and attending a social opportunity, during their return home, and even when they are not consciously using the app.

Proposed designs reflected three roles that social matching apps can assume for supporting risk management: 1) *the cloaking device* for maintaining discoverability to other users in the app, 2) *the informant* for helping users predict risk of a face-to-face meeting, and 3) *the guardian* for monitoring a user's safety status during face-to-face meetings and augmenting their response to potential or actualized harm. We unpack each role in the following subsections. See Table 2 for a summary of design concepts associated with each of the roles.

5.1 The Cloaking Device: Managing Visibility to Other Social Matching App Users

Participants often exemplified loss of risk control with indiscriminate discoverability of their profile and location in today's social matching apps that perform matching based on geographic proximity. They reflected with concern about increasing granularity of relative location (P15: *"This person's like 600 feet from me. This one's like 300 feet from you"*). Stalking was a recurrent fear, but more generally participants found it *"dangerous"* to have their location announced to any nearby person, especially when in areas that one is unfamiliar with. Some participants indicated that this loss of visibility control was a primary reason they discontinued use of some social matching apps.

P21: *"I also think this can be like, an easy way for stalkers to kind of get access to people or find out more information about people as well. […] Like I have a friend who has a stalker, and it's like, it's one of the scariest things in her life, whether or not like, he doesn't have bad intentions, at least we don't think so. But it is something that, like she worries about."*

P3: *"There was an app I used, I can't remember the name of it, but it would like, literally notify you in that instant if you're within one mile of someone else who had the app. And that's, that seems extremely dangerous to me. […] That was terrifying. I deleted it right away. It was like so I was walking on campus and getting notifications of like, this person is 50 feet from you, this person's like 300 feet from you. That's dangerous as like a woman."*

A design theme responsive to these concerns was management of profile visibility. Proposed designs varied based on who can view a user's profile, what parts of the profile are visible, and dynamic visibility management that is automated by AI.

Managing visibility of one's profile is already commonplace in current social matching apps, however participants proposed some key modifications/additions. Some wanted to limit their profile visibility to particular people, such as friends and known acquaintances who are nearby, or strangers with particular affinities (e.g., gender identity). This type of selective visibility is not

Table 2. Participants' social matching app design concepts organized according to the three overarching roles for risk management

Social Matching App Role	Design Concepts	Description and Sub-Design Concepts
Cloaking Device	Selective profile visibility	Limit discoverability of profile to specific people (e.g., preexisting contacts, users with specific affinities like gender identity)
	Manually control visibility of parts of profile	Enabling users to discover one's profile but with sensitive elements being invisible by default (e.g., their full name, age). Users would toggle the visibility of profile elements for particular partners at their discretion.
	AI-driven dynamic profile visibility	Leverages contextual information such as crime rate of geographic area, time of day
Informant	Crowdsourced risk awareness	- Risk awareness AI informed by privately provided reviews of in-person meeting partners - Publicly available reviews of a user from their past meeting partners - Multi-person social opportunities to crowdsource information between current and prospective attendees
	Location verification	Meeting partner takes picture of meeting location to ensure its legitimacy
	Emergency facilities	App informs users of emergency facilities near their meeting location
Guardian	"Friends & family" standby systems	User provides list of trusted contacts and predefined rules for alerting them before meeting stranger face-to-face. - Trusted contacts can access real time location monitoring - Trusted contacts auto-alerted of suspicious location patterns
	Recurrent safety check ins	App recurrently checks in with user about safety status during face-to-face meeting. - Explicit push notification asking about safety status - Covert check ins through "safe words" and "fake" text messages
	"I feel unsafe" button	Broader intent for use than traditional "panic" button. User proactively tells app to alert trusted contacts… - about general discomfort before emergency actually occurs - for assistance leaving a meeting location where they feel unsafe
	Confirming safe return home	- App alerts user of suspicious location patterns of meeting partner while they are returning home that could indicate stalking - "Safe word" inputted in app to confirm safe return

present in current social matching apps, which give simple dichotomous choices of whether to be visible to everyone or visible to none. Other participants considered toggling profile visibility on the basis of geographic area. According to P11: *"Like, if you're in an area where you don't want your profile to show up […] then you can hide that as well. So you don't delete it, but it's just not visible to anyone."* Some participants suggested that the matching app's AI could manage dynamic visibility on their behalf, freeing users from having to actively manage their visibility throughout the day. Participants considered various contextual factors that could inform the AI's visibility decisions such as crime rate of the surrounding area and presence of potential bystanders who

Fig. 2. P7 proposed a design that lets users toggle visibility of specific parts in their profile.

could intervene in harm. Participants that identified with an ethnic minority were particularity interested in dynamic location-based visibility, referencing towns and areas that are less tolerant of racial diversity.

An alternative approach to managing discoverability to other users was managing visibility of particular parts of one's profile (Figure 2). Location was a frequent suggestion, which is a currently present feature in social matching apps for men seeking men such as Grindr. Participants wanted to extend this functionality to other profile information such as their gender identity, age, and any other information that one might not want the entire userbase to know. One of the more interesting elements that participants suggested adding to profiles and making selectively visible was their full name that matches their *"government ID."* Participants described toggling their full name and other hidden parts of their profile "on" for specific partners before a face-to-face meeting, therefore affording one's partner the ability to better predict risk associated with themselves (in recognition that they themselves could be considered risky to prospective meeting partners).

5.2 The Informant: Augmenting Awareness of Risk Before Attending a Face-to-Face Encounter

Choosing to meet a social matching app user face-to-face is a significant decision because it simultaneously introduces susceptibility to physical harm while reducing one's capacity to manage risk. Many participants thus focused on ways that a social matching app could augment users' awareness of risk before venturing "off the app" into a face-to-face encounter with strangers. In addition to profile picture verification as implemented in several social matching apps, participants suggested that users could also upload pictures of face-to-face meeting locations to help users confirm that the meeting location is legitimate. Participants also suggested that social matching apps could inform users of nearby emergency facilities, in addition to general phone hotlines already provided for reporting harm, so they can better assess available resources for managing harm during a face-to-face encounter.

Yet a majority of design concepts for augmenting awareness of risk leveraged collective action of the userbase; they envisioned a social matching app that coordinates the broader userbase in working together to keep each other safe. We discuss two of the more frequent collective action-based ideas below.

5.2.1 User Reviews and Risk Prediction AI. One design idea that was proposed across all participatory design groups was providing reviews or ratings about users that one previously met face-to-face through the app. Some participants anticipated these reviews being private, and only accessible by AI to inform a risk prediction model. Participants envisioned the app sending *"safety alerts"* to users about a person discovered on the app when past reviews indicate that they may pose danger. In the words of P1: *"Like a safety alert sort of thing like if [...] there are multiple reviews on that maybe the system kind of looks for that and gives you like a pop-up alert before you even go on their page so that you know when that comes up."*

Other participants wanted direct access to reviews of other users through a *"review section"* on profiles so that they could manually predict risk of a potential meeting partner. They did acknowledge possibility for manipulation or adverse effects of public user reviews, such as repeated negative reviews in retaliation for a bad date/meeting or orchestration of multiple positive reviews. According to P11: *"Someone might try to like, kind of hack the system and have like, all their friends vote for them. So they have like the superior rating."* To address this potential misuse, participants suggested restricting the number of reviews one could submit about a particular user, clarifying that reviews should specifically be about safety, and restricting who can write reviews only to those who have actually met a particular user face-to-face; this could be confirmed with QR code scanning and location image verification as mentioned above.

5.2.2 Multi-Person Social Opportunity Profiles and Group Chat. Participants exhibited much interest in discovery of group activities and multi-person social opportunities in future social matching apps, in addition to profiles for individual people as typical in dating apps today. See a participant-generated mockup of a multi-person social opportunity profile in Figure 3. They contrasted the inherent risk management afforded by having bystanders (other attendees) able to intervene in unsafe situations with the *"aloneness"* of face-to-face meetings with an individual person. But in addition to bystander interventions while attending group-based social meetups, participants also envisioned bystander intervention in decisions to attend a face-to-face social opportunity in the first place. One idea that amassed support from several participants was a group chat related to a multi-person social opportunity profile discovered in the social matching app. Participants envisioned using the group chat to communicate with attendees who are already physically present at the social opportunity to assess risk. Some made a distinction between chat with the activity *"host"* or organizer, who would presumably be most capable of providing real-time risk assessment to prospective attendees, and other people who are attending.

P6:*"I was thinking like the chat with the host that you'd have open from before meeting up that would still be open like in case one of the people there like one of the other people who came to the event is being suspicious. And on the flip side of that the group chat with the other people there in case the host is the one being suspicious."*

P7: *"There will also be a little message button right underneath your picture if you want to say message to host or maybe message actually [...] whoever else is attending."*

Participants' designs also involved crowdsourcing visual evidence of social opportunities so that prospective attendees could confirm the validity of group chat comments and arrive at their own conclusion about risk of attendance. P8 envisioned these pictures being provided by the social opportunity host, while other participants suggested that pictures could be regularly updated by the host or others to give prospective attendees a glimpse at the activity's current state.

P5: *"It there's an image at the top that I would imagine would be taken by the host of the event. So, it could be a picture of the spot in the library where they're sitting at or like a little placard on the table that people should be looking for."*

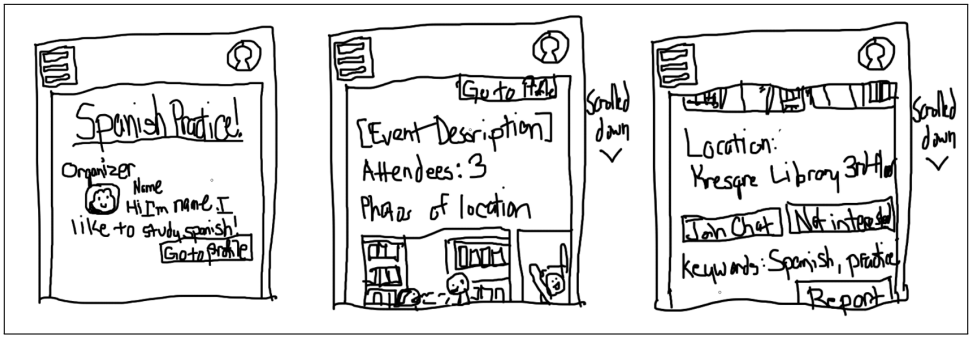

Fig. 3. These mockups depict a profile page for a multi-person social activity ("Spanish practice"), which participants encouraged because they can provide inherent risk management through availability of bystanders. The middle mockup depicts photos of the activity location that would have been uploaded by the activity host or other attendees, and the mockup on the right features a button to join a group chat with other users who are already attending the activity and could provide real-time updates for risk assessment.

5.3 The Guardian: Augmenting Women's Existing Safety Strategies During Face-to-Face Encounters

Another common focal point in participants' designs was on how the social matching app could help women manage imminent or actualized harm during face-to-face encounters. Several expected the social matching app to augment the safety strategies that women already practice while meeting strangers face-to-face. Participants typically referred to a *"check in"* strategy that entails notifying trusted contacts of their decision to meet (e.g., go on a date) with a social matching app user, including where and when the meeting is occurring, and then repeatedly checking in with their trusted contact through text messages or phone calls and alerting them should assistance be needed. P17 described use of the strategy for managing risk of kidnapping:

"Kidnapping is like one of my, like, biggest fears on a date. That's why I mentioned earlier, I always text my best friend and let her know where I'm going to be, what's his name, who I'm going to be with. If I can send a photo of him. And then let her know like, what time I'm going to be home."

A theme behind several proposed designs was automation and more discrete support for the check in strategy by the social matching app. The social matching app would assume responsibility for *"keeping an eye out"* for the user's wellbeing and coordinating information sharing amongst trusted contacts. We break down proposed functionality for this role, which we dubbed "the guardian," into three phases: preparing for a face-to-face encounter, attending a face-to-face encounter, and returning home safely.

5.3.1 Preparing for a Face-to-Face Encounter. Prior to venturing off the app to meet a stranger face-to-face, participants suggested that users could establish a *"friends and family on standby"* system in the social matching app. This would include the identities and contact information for trusted contacts and predefined rules for when and how they should be contacted. The types of people that would represent trusted contacts varied amongst participants. Friends and family members were most frequently mentioned hence the suggested name of the system, and one even suggested employees of the social matching app company. Only a few mentioned law enforcement personnel, likely because they anticipated alerting trusted contacts for help prior to a crime actually occurring. Once the user is prepared to travel to the face-to-face meeting the social matching app would notify their trusted contacts of their plans in order to prepare them to be on alert should

assistance be needed, but also to help them anticipate when they should return home. According to P21:

"So the user of the app would put in a secondary contact [...] I could put in my sister who's in the area. And then when I go to an event my sister would receive a notification of '[participant's name] going to [meet this user] at 10 o'clock and the location is [location name]'."

5.3.2 Attending a Face-to-Face Encounter. Despite concerns about their real-time location being visible to other users (see section 5.1), participants encouraged the idea of their location being *"monitored"* by the social matching app while meeting other users face-to-face. They *"felt safer having themselves tracked"* in the words of P15, because their location data could inform automatic alerts to their trusted contacts. For example, if a user's location indicates that they have stayed at the face-to-face meeting spot for longer than expected, or had a sudden change of location that did not align with expected duration of the meeting, the app would be triggered to notify one's trusted contacts.

P3: *"You could set it to like, track you in the location of the event. And if something were to happen, where if you leave the event without notifying the app that you're leaving, it could like send a message to an emergency contact."*

In addition to automatic location-based alerts to trusted contacts, participants also suggested that the app could repeatedly check in with them to confirm their safety status. Some envisioned this occurring through push notifications that directly asked about their safety, while others suggested more discrete ways of checking in so that their face-to-face meeting partners would not become aware. One idea that garnered approval from several participants was the app impersonating a parent or friend and sending a *"fake"* text message or phone call to solicit input from the user about their safety status. The content of such text messages would not overtly be about safety, but rather an unrelated topic that the user could pre-designate in the interface. In P15's words: *"The system could either send you a fake call or fake text, asking like 'Hey, are you safe?' [It could] pretend to be your parent or your significant other, making sure that you're feeling okay. And it could randomize [...] the safe word."*

Likewise, users could direct the app to alert their emergency contacts by inputting a *"safe word"* or phrase that does not have an obvious safety connotation to meeting partners.

Lastly, participants also wanted the ability to proactively direct the app to alert their trusted contacts. Multiple participants designed for this with an *"I feel unsafe"* button; wording that was deliberately chosen to reflect diverse reasons for alerting trusted contacts other than when harm is actually occurring. Some wanted to notify their trusted contacts to generally be on alert, or because they are uncomfortable and want some assistance with leaving before harm occurs. P22 described using the button to alert an employee of the social matching app company to call them on the phone with an excuse to leave the social encounter:

P21: *"Like if you feel unsafe you can possibly press a button to like alert an employee from the app to like know that okay, this person feels unsafe I will call them. So they create like you know like kind of like a fake call almost so that you could say 'oh, I have to go' like to the other person and then you stay on the phone with the safety employee."*

5.3.3 Returning Home Safely. In participants' designs they expected the social matching app to continue monitoring their location and checking in with them after they left a social encounter until they arrived safely back home (see Figure 4 for examples). To help users best assess if they are truly safe the app would inform them if the relative location of a meeting partner is still nearby after they have returned home, which could be indicative of stalking. As P5 described: *"So, say you attended an event. And maybe there was somebody there that was a little bit creepy, maybe into you,*

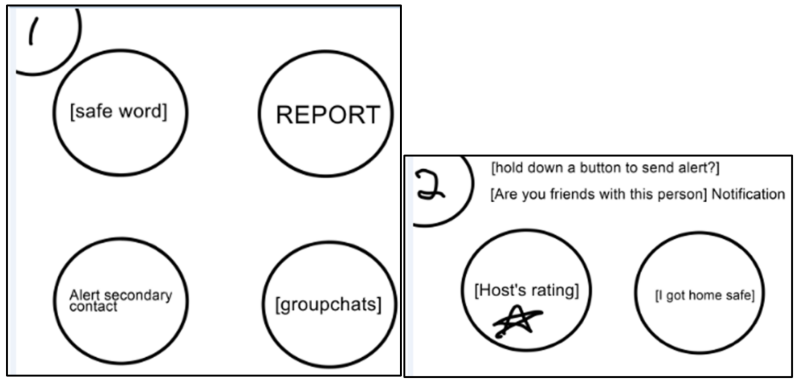

Fig. 4. P11's interfaces demonstrated two different approaches to confirming with the social matching app that one has returned home safely. One (right) involves the user clicking an "I got home safe" button, whereas the interface on the left enables users to input a "safe word" which only they would know, therefore preventing a stalker or perpetrator of harm from erroneously indicating that the user is safe.

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."

When confirming their return home, some participants suggesting inputting a *"safe word"* into the app rather than simply clicking a button. Unlike use of a safe word during face-to-face encounters for covertly updating the app, the use of a safe word when returning home was suggested to prevent malicious actors from stealing a user's phone and erroneously reporting their safe return.

6 DISCUSSION

In this paper we presented a participatory design study with 22 women in the United States about how mobile social matching apps could be designed to foreground safety. Findings emphasize that women in the study do not want to be "protected" by social matching apps, but rather augmented in their abilities for self-protection. Safety was conceptualized as the power to manage risk of harm associated with meeting other users-face-to-face, which participants illustrated with three new roles for social matching apps: 1) the cloaking device for managing discoverability to other users, 2) the informant for predicting risk of a particular social opportunity, and 3) the guardian for monitoring a user's safety status and augmenting response to potential or actualized harm in face-to-face settings.

The findings can be valuable in charting a course for future safety-conscious design of online-to-offline social experiences, however we do not necessarily advocate for the implementation of all participants' proposed designs. In this section we reflect on the anticipated positive and negative implications of the design concepts, organized around the three overarching design themes from the findings. By doing so we delineate the specific design concepts proposed by participants from the underlying unmet safety needs that they are intended to address.

6.1 Managing Risk Through Visibility: Discussion of "The Cloaking Device"

The proposed designs involving management of one's discoverability to other users (collectively dubbed "the cloaking device") reinforce positions of prior work that simply being a user of a social matching app poses risk to marginalized groups through their discoverability to other users and disclosure of their marginalized status [12, 35, 46, 71]. As mentioned in the Background, some affordances for profile visibility management already exist in social matching apps, however they

do not accommodate our participants' needs for dynamic visibility management that comprise the cloaking device theme.

Users are typically able to manually turn off discoverability of their profile in most social matching apps today. However, repurposing this feature for dynamic and frequent toggling of discoverability based on one's surroundings (which participants desired) carries significant usability issues. Users may forget to toggle their visibility off or on when their context changes, which could be quite frequent, thus rendering the feature rather unusable except for taking an extended break from the app [47]. Participants did propose alternative visibility management designs that could reduce this burden. One was allowing users to set guidelines ahead of time on the types of users they want to be discoverable to, such as those with the same gender or with shared affinities that the user thinks may reduce risk of harm. Another was AI-driven dynamic visibility management based on contextual data, although users would need to be involved in training and oversight of the AI to ensure it is making users (in)visible as expected. We consider both of these options to be worthy of further research and design.

Some participants also proposed setting sensitive elements of their profile as invisible by default and then toggling their visibility on for particular users they are about to meet face-to-face (in an effort to help their partner evaluate risk of meeting them). This would expand the functionality of the "hide distance" feature currently present in Grindr and other apps, albeit with the ability to toggle visibility for specific partners instead of the entire user base, and for more elements of the profile. Women's desire for control over granular elements of their profile draws parallels to self-disclosure considerations exhibited by other marginalized groups, particularly in terms of disabilities [71], transgender status [35], and HIV/STI status [103]. Setting aside concerns that researchers have already expressed about hiding location from one's profile [21, 49], an interface affordance for toggling visibility of several different profile elements could impose social pressure to disclose all of one's profile before any face-to-face meeting (e.g., it might make their partner think they have something to hide if they leave some elements hidden). Prior work regarding authenticity on social media demonstrates that this could be costly and anxiety-inducing for women and other marginalized groups who rely on strategic self-disclosure for privacy [29, 44]. Accordingly, we do not advocate for this approach.

6.2 Managing Risk Through Collective User Experience: Discussion of "The Informant"

Use of social matching apps today is largely a private experience. One typically evaluates a new user profile alone, they interact with users one-on-one in a private messaging interface, and they meet other users in the physical world for one-on-one meetings and dates. This private user experience affords minimal ability to predict risk of harm beyond information that the partner directly provides (and controls), with exception of search engine results or public social media profiles [40]. Several designs proposed by our participants sought to reframe social matching app-use as a collective experience in which users can rely on each other for risk awareness and response. These designs could be considered computer-mediated implementations of bystander intervention, a strategy promoted in public health for harm prevention [62], and which has received some support from a prior lab study of safety app designs [52]. Whereas bystander intervention is traditionally framed as a reactive measure (a bystander intervening in harmful or harassing behavior that they observe occurring against another person), the computer-mediated interventions proposed by our participants were more preemptive – other users would assist one in avoiding a harmful situation altogether.

There were two design concepts proposed by participants that demonstrate this preemptive form of bystander intervention. One, which we personally advocate to future designers and researchers, is app support for multi-user social opportunity profiles such as group activities and gatherings. Other

people attending the social opportunity can act as bystanders in the traditional reactive sense, and they can also intervene preemptively as participants illustrated with designs for group chats between current and prospective attendees at a social gathering. For example, participants already attending a social gathering at a bar could inform prospective attendees in a group chat of a belligerent or harassing person. Social matching apps have been slow to explicitly accommodate multi-person profiles. The growing accommodation for myriad individualized social goals [32, 50, 94, 95] suggests it may be time to revisit the types of social opportunities supported through app design for safety purposes.

Another—more controversial—design proposal for bystander intervention involved materializing past experiences with meeting partners through user reviews/ratings. The additional data this could provide to women for predicting risk of harm may be valuable, yet our participants themselves were also quick to critique the feature for its susceptibility to misuse. Users could receive negative reviews in retaliation for a rejected sexual advance (see other evidence of retaliatory harassment in Tinder [82]), or users could have their friends leave fake positive reviews. Even if users leave reviews in earnest they could be susceptible to racial bias, which seems quite likely given the known racial bias in how users review profiles [48]. There is also the question of how new users may be adversely impacted by simply not having reviews. If reviews of products on e-commerce websites are any indication [26], user reviews could widen the gap in attention between already-popular users and those that struggle to receive matches while furthering the objectification of users [84]. This of course assumes that users will actually provide reviews on their meeting/interaction partners, which may be a misassumption in light of prior work indicating that women seldom use the reporting functionality already available in dating apps [74]. Given concerns of misuse, bias, and doubts over whether the broader userbase would even use the feature, we advocate against the implementation of user review functionality while still recognizing the merits of our participants' underlying reason for proposing the feature: to increase available information for predicting and avoiding risk of harm.

6.3 Managing Risk Through Location Tracking: Discussion of "The Guardian"

Participants in our study directed much attention to use or presence of social matching apps during face-to-face encounters for risk management. Their ideas join a growing body of HCI work that seeks just-in-time intervention into physical harms such as sexual assault and street harassment [2, 65, 68, 77].

Some participants' ideas in this area centered on continuous location tracking, which they were surprisingly open to because it would allow trusted contacts to monitor their whereabouts and react quickly to requests for assistance. In practice however constant location sharing may expose users to data vulnerabilities and other unintended uses of their granular location data by third parties [58, 87]. Some participants also advocated for constant location tracking of their meeting partners after a face-to-face meeting has ended so that the social matching app could identify stalking patterns (e.g., following a woman home). This raises serious questions about how a social matching app may distinguish nefarious from coincidental reasons for remaining in a user's vicinity. There is potential to inadvertently create risk if a user's location is shared without their consent because the app has incorrectly determined them to be a stalker. In light of a growing advocacy around consentful technology [51, 55, 112] and concerns around nonconsensual collection and use of data through social media [108] we cannot advocate for designs hinging on continuous location tracking no matter the anticipated safety benefits.

This does not mean that social matching apps should not play a role during face-to-face meetings at all. Participants also proposed designs that leveraged location in less invasive ways, particularly an "I feel unsafe" button that would collect one's location and alert trusted contacts at the particular

moment it is clicked. Such a feature would reduce the extent of location tracking and would leave the decision in the user's hands about when their location is captured and conveyed to others. At first glance the "I feel unsafe" button may seem redundant with the "panic" button that has pervaded the literature [53] and public policy [86], and been incorporated into mobile applications including modern day social matching apps [96]. However there are key differences that lead us to advocate for the "I feel unsafe" button being incorporated into future designs. Panic buttons as currently implemented are intended for use when harm is already occurring, which limits utility of the button as a preventative measure, as well as a user's ability to trigger it if they are incapacitated by an attacker. Empirical insight into women's perspectives on implementation of panic buttons in India following a highly publicized gang rape can be found in [53]. Furthermore, the recipients of panic button alerts are typically law enforcement personnel. This imposes boundaries on what qualifies as an emergency and reason to click the panic button. If one feels generally uncomfortable, at risk of imminent harm, or otherwise afflicted by a harm that would not be considered a crime then law enforcement would not be the appropriate personnel to contact. In contrast, our participants' vision for an "I feel unsafe" button maintains user agency in who is alerted, and why. This expands potential uses of the button beyond reaction to criminal activity and can enable prevention of harm by alerting trusted contacts preemptively to help them eject from a risky situation.

7 CONCLUSION

This study is motivated by a growing body of evidence about social matching and dating app-facilitated harms, and disproportionate victimization on the basis of gender. We conducted a participatory design study with 22 women in the Midwest United States to develop understanding of how social matching apps could be designed to better foreground their safety. Doubting the feasibility of social matching apps being able to completely eliminate risk of harm, proposed designs sought to augment women's own abilities for self-protection through increased awareness and management of risk. Proposed designs reflected three roles that social matching apps can assume pursuant to risk management: 1) the cloaking device for managing discoverability to other users, 2) the informant for predicting risk of a particular social opportunity, and 3) the guardian for monitoring a user's safety status and augmenting response to risk during face-to-face meetings. The study informs a future course for safety-conscious design by extending the use of social matching apps into face-to-face encounters and providing users with more information to assess risk.

8 ACKNOWLEDGMENTS

We thank Caroline Bull, Isha Datey, Jonathan Sienkiewicz, Alexander Gamache, Joseph Prizlow, Kyle McBride, Jakob Welchner, and Caleb White for assisting in preparations for this paper. We also thank Kelly Berishaj, Michele Parkhill Purdie, and Melissa McDonald for invaluable insight that informed this study's design. The constructive feedback from anonymous reviewers of this paper is also much appreciated. This material is based upon work partially supported by the U.S. National Science Foundation under Grant No. IIS-2211896.

REFERENCES

[1] UK National Crime Agency. 2016. Emerging new threat in online dating - Initial trends in internet dating-initiated serious sexual assaults. *National Crime Agency* (2016). https://trends.ifla.org/node/425

[2] Syed Ishtiaque Ahmed, Steven J Jackson, Nova Ahmed, Hasan Shahid Ferdous, Md Rashidujjaman Rifat, A S M Rizvi, Shamir Ahmed, and Rifat Sabbir Mansur. 2014. Protibadi: A platform for fighting sexual harassment in urban Bangladesh. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2695–2704.

[3] Kath Albury, Paul Byron, Anthony McCosker, Tinonee Pym, Jarrod Walshe, Kane Race, Doreen Salon, Tim Wark, Jessica Botfield, Daniel Reeders, and Christopher Dietzel. 2019. Safety, risk and wellbeing on dating apps: Final report. (2019). https://doi.org/10.25916/5dd324c1b33bb

[4] Mohammed Eunus Ali, Shabnam Basera Rishta, Lazima Ansari, Tanzima Hashem, and Ahamad Imtiaz Khan. 2015. SafeStreet: empowering women against street harassment using a privacy-aware location based application. *Proceedings of the Seventh International Conference on Information and Communication Technologies and Development*, 1–4.

[5] Nazanin Andalibi, Oliver L Haimson, Munmun De Choudhury, and Andrea Forte. 2016. Understanding social media disclosures of sexual abuse through the lenses of support seeking and anonymity. *Proceedings of the 2016 CHI conference on human factors in computing systems*, 3906–3918.

[6] Monica Anderson, Emily A. Vogels, and Erica Turner. 2020. The virtues and downsides of online dating. https://www.pewresearch.org/internet/2020/02/06/the-virtues-and-downsides-of-online-dating/

[7] Jeffrey Bardzell, Shaowen Bardzell, and Lone Koefoed Hansen. 2015. Immodest Proposals: Research Through Design and Knowledge. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2093–2102. https://doi.org/10.1145/2702123.2702400

[8] Shaowen Bardzell. 2010. Feminist HCI: taking stock and outlining an agenda for design. *Proceedings of the SIGCHI conference on human factors in computing systems*, 1301–1310.

[9] Laura Beckwith, Cory Kissinger, Margaret Burnett, Susan Wiedenbeck, Joseph Lawrance, Alan Blackwell, and Curtis Cook. 2006. Tinkering and gender in end-user programmers' debugging. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 231–240. https://doi.org/10.1145/1124772.1124808

[10] Andrew B. L. Berry, Catherine Y. Lim, Tad Hirsch, Andrea L. Hartzler, Linda M. Kiel, Zoë A. Bermet, and James D. Ralston. 2019. Supporting Communication About Values Between People with Multiple Chronic Conditions and their Providers. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–14. https://doi.org/10.1145/3290605.3300700

[11] Jeremy Birnholtz, Colin Fitzpatrick, Mark Handel, and Jed R Brubaker. 2014. Identity, identification and identifiability: The language of self-presentation on a location-based mobile dating app. *Proc. MobileHCI 2014*, 3–12. https://doi.org/10.1145/2628363.2628406

[12] Jeremy Birnholtz, Shruta Rawat, Richa Vashista, Dicky Baruah, Alpana Dange, and Anne-Marie Boyer. 2020. Layers of Marginality: An Exploration of Visibility, Impressions, and Cultural Context on Geospatial Apps for Men Who Have Sex With Men in Mumbai, India. *Social Media+ Society* 6 (2020), 2056305120913995. Issue 2.

[13] Jeremy Birnholtz, Irina Shklovski, Mark Handel, and Eran Toch. 2015. Let's talk about sex (Apps), CSCW. *Proceedings of the 18th ACM Conference Companion on Computer Supported Cooperative Work Social Computing*, 283–288.

[14] Ginette C. Blackhart, Jennifer Fitzpatrick, and Jessica Williamson. 2014. Dispositional factors predicting use of online dating sites and behaviors related to online dating. *Computers in Human Behavior* 33 (2014), 113–118. https://doi.org/10.1016/j.chb.2014.01.022

[15] 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 Society* (2014), 1–20. https://doi.org/10.1177/1461444814521595

[16] Jan Blom, Divya Viswanathan, Mirjana Spasojevic, Janet Go, Karthik Acharya, and Robert Ahonius. 2010. Fear and the city: role of mobile services in harnessing safety and security in urban use contexts. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1841–1850.

[17] Virginia Braun, Victoria Clarke, Nikki Hayfield, and Gareth Terry. 2019. Thematic Analysis. , 843-860 pages. https://doi.org/10.1007/978-981-10-5251-4_103

[18] Samantha Breslin and Bimlesh Wadhwa. 2014. Exploring Nuanced Gender Perspectives within the HCI Community. *Proceedings of the India HCI 2014 Conference on Human Computer Interaction - IHCI '14*, 45–54. https://doi.org/10.1145/2676702.2676709

[19] Margaret Burnett, Anicia Peters, Charles Hill, and Noha Elarief. 2016. Finding Gender-Inclusiveness Software Issues with GenderMag: A Field Investigation. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 2586–2598. https://doi.org/10.1145/2858036.2858274

[20] David M. Buss and David P. Schmitt. 1993. Sexual strategies theory: An evolutionary perspective on human mating. *Psychological review* 100 (1993), 204–232. Issue 2. https://doi.org/10.1037/0033-295X.100.2.204

[21] Vanessa Centelles, Ráchael A. Powers, and Richard K. Moule. 2021. An Examination of Location-Based Real-Time Dating Application Infrastructure, Profile Features, and Cybervictimization. *Social Media + Society* 7 (7 2021), 205630512110432. Issue 3. https://doi.org/10.1177/20563051211043218

[22] 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. *Sexual Abuse* 30 (2018), 343–366. Issue 4.

[23] Elizabeth F. Churchill. 2010. Sugared puppy-dog tails: gender and design. *Interactions* 17 (3 2010), 52–56. Issue 2. https://doi.org/10.1145/1699775.1699787

[24] Francesca Comunello, Lorenza Parisi, and Francesca Ieracitano. 2020. Negotiating gender scripts in mobile dating apps: between affordances, usage norms and practices. *Information, Communication Society* (2020), 1–17.

[25] Danielle Couch and Pranee Liamputtong. 2008. Online dating and mating: The use of the internet to meet sexual partners. *Qual.Health Res* 18 (2008), 268–279. Issue 2. https://doi.org/18/2/268[pii];10.1177/1049732307312832[doi]

[26] Geng Cui, Hon-Kwong Lui, and Xiaoning Guo. 2012. The Effect of Online Consumer Reviews on New Product Sales. *International Journal of Electronic Commerce* 17 (10 2012), 39–58. Issue 1. https://doi.org/10.2753/JEC1086-4415170102

[27] Yichao Cui, Naomi Yamashita, Mingjie Liu, and Yi-Chieh Lee. 2022. "So Close, yet So Far": Exploring Sexual-minority Women's Relationship-building via Online Dating in China. *CHI Conference on Human Factors in Computing Systems*, 1–15. https://doi.org/10.1145/3491102.3517624

[28] Michael A. DeVito, Jeremy Birnholtz, and Jeffery T. Hancock. 2017. Platforms, People, and Perception: Using Affordances to Understand Self-Presentation on Social Media. *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, 740–754. https://doi.org/10.1145/2998181.2998192

[29] Alexander Dhoest and Lukasz Szulc. 2016. Navigating Online Selves: Social, Cultural, and Material Contexts of Social Media Use by Diasporic Gay Men. *Social Media + Society* 2 (10 2016), 205630511667248. Issue 4. https://doi.org/10.1177/2056305116672485

[30] Catherine D'Ignazio, Alexis Hope, Becky Michelson, Robyn Churchill, and Ethan Zuckerman. 2016. A Feminist HCI Approach to Designing Postpartum Technologies: "When I first saw a breast pump I was wondering if it was a joke". *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 2612–2622. https://doi.org/10.1145/2858036.2858460

[31] Jill P Dimond, Michaelanne Dye, Daphne LaRose, and Amy S Bruckman. 2013. Hollaback! The role of storytelling online in a social movement organization. *Proceedings of the 2013 conference on Computer supported cooperative work*, 477–490.

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

[33] Nicole Ellison, Rebecca Heino, and J. L. Gibbs. 2006. Managing impressions online: self-presentation processes in the online dating environment. *Journal of Computer-Mediated Communication* 11 (2006), 415–441. https://doi.org/10.1111/j.1083-6101.2006.00020.x

[34] Jody Farnden, Ben Martini, and Kim-Kwang Raymond Choo. 2015. Privacy risks in mobile dating apps. *arXiv preprint arXiv:1505.02906* (2015).

[35] Julia R. Fernandez and Jeremy Birnholtz. 2019. "I Don't Want Them to Not Know": Investigating Decisions to Disclose Transgender Identity on Dating Platforms. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 226 (nov 2019), 21 pages. https://doi.org/10.1145/3359328

[36] Andrea Forte, Judd Antin, Shaowen Bardzell, Leigh Honeywell, John Riedl, and Sarah Stierch. 2012. Some of all human knowledge: Gender and Participation in Peer Production. *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work Companion*, 33–36. https://doi.org/10.1145/2141512.2141530

[37] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3173574.3174241

[38] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW, Article 46 (dec 2017), 22 pages. https://doi.org/10.1145/3134681

[39] Claudia Garcia-Moreno, Christina Pallitto, Karen Devries, Heidi Stöckl, Charlotte Watts, and Naeema Abrahams. 2013. *Global and regional estimates of violence against women: prevalence and health effects of intimate partner violence and non-partner sexual violence.* World Health Organization.

[40] Jennifer L Gibbs, Nicole B Ellison, and Chih-Hui Lai. 2010. First comes love, then comes Google: An investigation of uncertainty reduction strategies and self-disclosure in online dating. *Communication Research* 38 (2010), 70–100. Issue 1.

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

[42] Rosalie Gillett. 2018. Intimate intrusions online: Studying the normalisation of abuse in dating apps. *Women's Studies International Forum* 69, 212–219.

[43] Oliver L. Haimson, Dykee Gorrell, Denny L. Starks, and Zu Weinger. 2020. Designing Trans Technology: Defining Challenges and Envisioning Community-Centered Solutions. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13. https://doi.org/10.1145/3313831.3376669

[44] Oliver L. Haimson, Tianxiao Liu, Ben Zefeng Zhang, and Shanley Corvite. 2021. The Online Authenticity Paradox: What Being "Authentic" on Social Media Means, and Barriers to Achieving It. *Proceedings of the ACM on Human-Computer Interaction* 5 (10 2021), 1–18. Issue CSCW2. https://doi.org/10.1145/3479567

[45] Mark J Handel and Irina Shklovski. 2012. Disclosure, ambiguity and risk reduction in real-time dating sites. *Proceedings of the 17th ACM international conference on Supporting group work*, 175–178.

[46] Jean Hardy and Silvia Lindtner. 2017. Constructing a Desiring User: Discourse, Rurality, and Design in Location-Based Social Networks. *Proceedings of the ACM Conference on Computer-Supported Cooperative Work Social Computing - CSCW'17* (2017). https://doi.org/10.1145/2998181.2998347

[47] Nicola Henry and Anastasia Powell. 2018. Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, violence, abuse* 19 (2018), 195–208. Issue 2.

[48] Günter J Hitsch, Ali Hortaçsu, and Dan Ariely. 2010. What makes you click? — mate preferences and matching outcomes in online dating. *Quantitative Marketing and Economics* 0449625 (2010), 1–37. https://doi.org/10.1007/s11129-010-9088-6

[49] Nguyen Phong Hoang, Yasuhito Asano, and Masatoshi Yoshikawa. 2017. Your neighbors are my spies: Location and other privacy concerns in GLBT-focused location-based dating applications. *2017 19th International Conference on Advanced Communication Technology (ICACT)*, 851–860. https://doi.org/10.23919/ICACT.2017.7890236

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

[51] Jane Im, Jill Dimond, Melody Berton, Una Lee, Katherine Mustelier, Mark S. Ackerman, and Eric Gilbert. 2021. Yes: Affirmative Consent as a Theoretical Framework for Understanding and Imagining Social Platforms. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 403, 18 pages. https://doi.org/10.1145/3411764.3445778

[52] Mike Just, Hasmeet Chandok, Raghav Sampangi, Kirstie Hawkey, Alette Willis, JeyaBalaji Samuthiravelu, Dilpreet Gill, and Michael Altair. 2019. Personal Safety App Effectiveness. *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–6. https://doi.org/10.1145/3290607.3312781

[53] Naveena Karusala and Neha Kumar. 2017. Women's safety in public spaces: Examining the efficacy of panic buttons in New Delhi. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 3340–3351.

[54] Os Keyes, Burren Peil, Rua M. Williams, and Katta Spiel. 2020. Reimagining (Women's) Health: HCI, Gender and Essentialised Embodiment. *ACM Transactions on Computer-Human Interaction* 27 (8 2020), 1–42. Issue 4. https://doi.org/10.1145/3404218

[55] Una Lee and Dan Toliver. 2017. Building Consentful Tech. http://www.consentfultech.io/wp-content/uploads/2019/10/Building-Consentful-Tech.pdf

[56] Amanda Lenhart, Michele Ybarra, Kathryn Zickuhr, and Myeshia Price-Feeney. 2016. *Online harassment, digital abuse, and cyberstalking in America.* Data and Society Research Institute.

[57] Dennis H. Li, Shruta Rawat, Jayson Rhoton, Pallav Patankar, Maria L. Ekstrand, B. R. Simon Rosser, and J. Michael Wilkerson. 2017. Harassment and Violence Among Men Who Have Sex with Men (MSM) and Hijras After Reinstatement of India's "Sodomy Law". *Sexuality Research and Social Policy* 14 (9 2017), 324–330. Issue 3. https://doi.org/10.1007/s13178-016-0270-9

[58] Christoph Lutz and Giulia Ranzini. 2017. Where Dating Meets Data: Investigating Social and Institutional Privacy Concerns on Tinder. *Social Media + Society* 3 (1 2017), 205630511769773. Issue 1. https://doi.org/10.1177/2056305117697735

[59] Xiao Ma, Emily Sun, and Mor Naaman. 2017. What happens in happn: The warranting powers of location history in online dating. *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, 41–50.

[60] Wookjae Maeng and Joonhwan Lee. 2022. Designing and Evaluating a Chatbot for Survivors of Image-Based Sexual Abuse. *CHI Conference on Human Factors in Computing Systems*, 1–21. https://doi.org/10.1145/3491102.3517629

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

[62] Sarah McMahon and Victoria L. Banyard. 2012. When Can I help? A Conceptual Framework for the Prevention of Sexual Violence Through Bystander Intervention. *Trauma, Violence, Abuse* 13 (1 2012), 3–14. Issue 1. https://doi.org/10.1177/1524838011426015

[63] Bonita C. Meyersfeld. 2012. The Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence. *International Legal Materials* 51 (2 2012), 106–132. Issue 1. https://doi.org/10.5305/intelegamate.51.1.0106

[64] Nabila Rezwana Mirza, Shareen Mahmud, Prosonna Hossain Nabila, and Nova Ahmed. 2016. Poster: Protibaadi: An Extended Solution to Deal with Sexual Harassment. *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services Companion*, 59.

[65] Manisha Mohan, Misha Sra, and Chris Schmandt. 2017. Technological interventions to detect, communicate and deter sexual assault. *Proceedings of the 2017 ACM International Symposium on Wearable Computers*, 126–129.

[66] Michael J Muller and Sarah Kuhn. 1993. Participatory design. *Commun. ACM* 36 (1993), 24–28. Issue 6.
[67] Mustafa Ozkaynak, Christina M. Sircar, Olivia Frye, and Rupa S. Valdez. 2021. A Systematic Review of Design Workshops for Health Information Technologies. *Informatics* 8 (5 2021), 34. Issue 2. https://doi.org/10.3390/informatics8020034
[68] Polianna Paim, Laura Sánchez García, and Elissandra Gabriela Pereira. 2020. NO to violence against any woman! *Proceedings of the 19th Brazilian Symposium on Human Factors in Computing Systems*, 1–6. https://doi.org/10.1145/3424953.3426645
[69] Hyanghee Park and Joonhwan Lee. 2021. Designing a Conversational Agent for Sexual Assault Survivors: Defining Burden of Self-Disclosure and Envisioning Survivor-Centered Solutions. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 634, 17 pages. https://doi.org/10.1145/3411764.3445133
[70] Jonathan Petrychyn, Diana C Parry, and Corey W Johnson. 2020. Building community, one swipe at a time: hook-up apps and the production of intimate publics between women. *Health Sociology Review* (2020), 1–15.
[71] John R Porter, Kiley Sobel, Sarah E Fox, Cynthia L Bennett, and Julie A Kientz. 2017. Filtered out: Disability disclosure practices in online dating communities. *Proceedings of the ACM on Human-Computer Interaction* 1 (2017), 87. Issue CSCW.
[72] Josie Povey, Michelle Sweet, Tricia Nagel, Anne Lowell, Fiona Shand, Jahdai Vigona, and Kylie M Dingwall. 2022. Determining Priorities in the Aboriginal and Islander Mental Health Initiative for Youth App Second Phase Participatory Design Project: Qualitative Study and Narrative Literature Review. *JMIR Formative Research* 6 (2 2022), e28342. Issue 2. https://doi.org/10.2196/28342
[73] Anastasia Powell and Nicola Henry. 2019. Technology-facilitated sexual violence victimization: Results from an online survey of Australian adults. *Journal of interpersonal violence* 34 (2019), 3637–3665. Issue 17.
[74] Urszula Pruchniewska. 2020. "I Like That It's My Choice a Couple Different Times": Gender, Affordances, and User Experience on Bumble Dating. *International Journal of Communication* 14 (2020), 18.
[75] Afsaneh Razi, Seunghyun Kim, Ashwaq Alsoubai, Gianluca Stringhini, Thamar Solorio, Munmun De Choudhury, and Pamela J. Wisniewski. 2021. A Human-Centered Systematic Literature Review of the Computational Approaches for Online Sexual Risk Detection. *Proceedings of the ACM on Human-Computer Interaction* 5 (10 2021), 1–38. Issue CSCW2. https://doi.org/10.1145/3479609
[76] 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 Science, Medicine and Pathology* (2020), 1–7.
[77] Sohini Roy, Abhijit Sharma, and Uma Bhattacharya. 2015. MoveFree: A ubiquitous system to provide women safety. *Proceedings of the Third International Symposium on Women in Computing and Informatics - WCI '15*, 545–552. https://doi.org/10.1145/2791405.2791415
[78] Jennifer D Rubin, Lindsay Blackwell, and Terri D Conley. 2020. Fragile Masculinity: Men, Gender, and Online Harassment. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–14.
[79] Nithya Sambasivan, Amna Batool, Nova Ahmed, Tara Matthews, Kurt Thomas, Laura Sanely Gaytán-Lugo, David Nemer, Elie Bursztein, Elizabeth Churchill, and Sunny Consolvo. 2019. "They Don't Leave Us Alone Anywhere We Go": Gender and Digital Abuse in South Asia. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–14. https://doi.org/10.1145/3290605.3300232
[80] Muhammad Yasir Sarosh, Muhammad Abdullah Yousaf, Mair Muteeb Javed, and Suleman Shahid. 2016. Mehfoozaurat: Transforming smart phones into women safety devices against harassment. *Proceedings of the Eighth International Conference on Information and Communication Technologies and Development*, 1–4.
[81] 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, Behavior, and Social Networking* 20 (12 2017), 727–734. Issue 12. https://doi.org/10.1089/cyber.2017.0279
[82] Frances Shaw. 2016. "Bitch I said hi": The Bye Felipe campaign and discursive activism in mobile dating apps. *Social Media+ Society* 2 (2016), 2056305116672889. Issue 4.
[83] Rushank Shetty, George Grispos, and Kim-Kwang Raymond Choo. 2021. Are You Dating Danger? An Interdisciplinary Approach to Evaluating the (In)Security of Android Dating Apps. *IEEE Transactions on Sustainable Computing* 6 (4 2021), 197–207. Issue 2. https://doi.org/10.1109/TSUSC.2017.2783858
[84] Gratiela Sion. 2019. Commodifying intimate relationships through geosocial networking mobile apps: data-driven dating, sexual sociality, and online body objectification. *J. Res. Gender Stud.* 9 (2019), 78.
[85] Sharon Smith, Jieru Chen, Kathleen Basile, Leah Gilbert, Melissa Merrick, Nimesh Patel, Margie Walling, and Anurag Jain. 2016. National Intimate Partner and Sexual Violence Survey: 2010-2012 State Report. (2016).
[86] Meher Soni. 2016. Rethinking the Challenge of Women's Safety in India's Cities. *ORF Issue Brie* 159 (2016), 1–8.

[87] Zahra Stardust, Rosalie Gillett, and Kath Albury. 2022. Surveillance does not equal safety: Police, data and consent on dating apps. *Crime, Media, Culture: An International Journal* (7 2022), 174165902211118. https://doi.org/10.1177/17416590221111827

[88] Elizabeth Stowell, Teresa K. O'Leary, Everlyne Kimani, Michael K. Paasche-Orlow, Timothy Bickmore, and Andrea G. Parker. 2020. Investigating Opportunities for Crowdsourcing in Church-Based Health Interventions. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–12. https://doi.org/10.1145/3313831.3376833

[89] Sindy R. Sumter, Laura Vandenbosch, and Loes Ligtenberg. 2017. Love me Tinder: Untangling emerging adults' motivations for using the dating application Tinder. *Telematics and Informatics* 34 (2017), 67–78. Issue 1. https://doi.org/10.1016/j.tele.2016.04.009

[90] Muhammad Uzair Tariq, Afsaneh Razi, Karla Badillo-Urquiola, and Pamela Wisniewski. 2019. A Review of the Gaps and Opportunities of Nudity and Skin Detection Algorithmic Research for the Purpose of Combating Adolescent Sexting Behaviors. , 90-108 pages. https://doi.org/10.1007/978-3-030-22636-7_6

[91] Melissa Qingqing Teng, James Hodge, and Eric Gordon. 2019. Participatory Design of a Virtual Reality-Based Reentry Training with a Women's Prison. *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–8. https://doi.org/10.1145/3290607.3299050

[92] Loren Terveen and David W McDonald. 2005. Social matching: A framework and research agenda. *ACM transactions on computer-human interaction (TOCHI)* 12 (2005), 401–434. Issue 3.

[93] Laura Thompson. 2018. "I can be your Tinder nightmare": Harassment and misogyny in the online sexual marketplace. *Feminism Psychology* 28 (2018), 69–89. Issue 1.

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

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

[96] Tinder. 2020. Tinder Introduces Safety-Focused Updates. *Tinder Blog* (2020). https://blog.gotinder.com/tinder-introduces-safety-updates/

[97] Amaury Trujillo and Maria Claudia Buzzi. 2016. Participatory User Requirements Elicitation for Personal Menopause App. *Proceedings of the 9th Nordic Conference on Human-Computer Interaction*, 1–6. https://doi.org/10.1145/2971485.2996737

[98] Anupriya Tuli, Surbhi Singh, Rikita Narula, Neha Kumar, and Pushpendra Singh. 2022. Rethinking Menstrual Trackers Towards Period-Positive Ecologies. *CHI Conference on Human Factors in Computing Systems*, 1–20. https://doi.org/10.1145/3491102.3517662

[99] Pieter Vandekerckhove, Marleen de Mul, Wichor M Bramer, and Antoinette A de Bont. 2020. Generative Participatory Design Methodology to Develop Electronic Health Interventions: Systematic Literature Review. *Journal of Medical Internet Research* 22 (4 2020), e13780. Issue 4. https://doi.org/10.2196/13780

[100] Kristin Veel and Nanna Bonde Thylstrup. 2018. Geolocating the stranger: the mapping of uncertainty as a configuration of matching and warranting techniques in dating apps. *Journal of Aesthetics Culture* 10 (8 2018), 43–52. Issue 3. https://doi.org/10.1080/20004214.2017.1422924

[101] George Veletsianos, Shandell Houlden, Jaigris Hodson, and Chandell Gosse. 2018. Women scholars' experiences with online harassment and abuse: Self-protection, resistance, acceptance, and self-blame. *New Media Society* 20 (12 2018), 4689–4708. Issue 12. https://doi.org/10.1177/1461444818781324

[102] Hao Wang, Congxing Cai, Andrew Philpot, Mark Latonero, Eduard H. Hovy, and Donald Metzler. 2012. Data integration from open internet sources to combat sex trafficking of minors. *Proceedings of the 13th Annual International Conference on Digital Government Research - dg.o '12*, 246. https://doi.org/10.1145/2307729.2307769

[103] Mark Warner, Andreas Gutmann, M Angela Sasse, and Ann Blandford. 2018. Privacy unraveling around explicit HIV status disclosure fields in the online geosocial hookup app Grindr. *Proceedings of the ACM on human-computer interaction* 2 (2018), 1–22. Issue CSCW.

[104] Mark Warner, Juan F Maestre, Jo Gibbs, Chia-Fang Chung, and Ann Blandford. 2019. Signal Appropriation of Explicit HIV Status Disclosure Fields in Sex-Social Apps used by Gay and Bisexual Men. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–15.

[105] Charlotte Watts and Cathy Zimmerman. 2002. Violence against women: global scope and magnitude. *The Lancet* 359 (4 2002), 1232–1237. Issue 9313. https://doi.org/10.1016/S0140-6736(02)08221-1

[106] Shangwei Wu and Janelle Ward. 2020. Looking for "interesting people": Chinese gay men's exploration of relationship development on dating apps. *Mobile Media Communication* 8 (2020), 342–359. Issue 3.

[107] Chaeyoon Yoo and Paul Dourish. 2021. Anshimi: Women's Perceptions of Safety Data and the Efficacy of a Safety Application in Seoul. *Proceedings of the ACM on Human-Computer Interaction* 5 (4 2021), 1–21. Issue CSCW1. https://doi.org/10.1145/3449221

[108] Jonathan Zong and J. Nathan Matias. 2022. Bartleby: Procedural and Substantive Ethics in the Design of Research Ethics Systems. *Social Media + Society* 8 (1 2022), 205630512210770. Issue 1. https://doi.org/10.1177/20563051221077021

[109] Douglas Zytko, Nicholas Furlo, Bailey Carlin, and Matthew Archer. 2021. Computer-Mediated Consent to Sex: The Context of Tinder. *Proceedings of the ACM on Human-Computer Interaction* 5 (2021), 27. Issue CSCW1. https://doi.org/10.1145/3449288

[110] Douglas Zytko, Sukeshini A. Grandhi, and Quentin Jones. 2014. Impression management struggles in online dating. *Proceedings of the 18th international conference on supporting group work*, 53–62. https://doi.org/10.1145/2660398.2660410

[111] Douglas Zytko, Sukeshini A Grandhi, and Quentin Jones. 2015. Frustrations with Pursuing Casual Encounters through Online Dating. *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*, 1935–1940. https://doi.org/10.1145/2702613.2732905

[112] Douglas Zytko, Jane Im, and Jonathan Zong. 2022. Consent: A Research and Design Lens for Human-Computer Interaction. In *Companion Publication of the 2022 Conference on Computer Supported Cooperative Work and Social Computing* (Virtual Event, Taiwan) *(CSCW'22 Companion)*. Association for Computing Machinery, New York, NY, USA, 205–208. https://doi.org/10.1145/3500868.3561201

[113] Douglas Zytko, Nicholas Mullins, Shelnesha Taylor, and Richard H. Holler. 2022. Dating Apps Are Used for More Than Dating: How Users Disclose and Detect (Non-)Sexual Interest in People-Nearby Applications. *Proc. ACM Hum.-Comput. Interact.* 6, GROUP, Article 30 (jan 2022), 14 pages. https://doi.org/10.1145/3492849

[114] Douglas Zytko, Victor Regalado, Nicholas Furlo, Sukeshini A. Grandhi, and Quentin Jones. 2020. Supporting Women in Online Dating with a Messaging Interface that Improves their Face-to-Face Meeting Decisions. *Proceedings of the ACM on Human-Computer Interaction* 4 (2020). Issue CSCW2. https://doi.org/10.1145/3415208

Received May 2022; revised August 2022; accepted September 2022