Toward a Feminist Social Media Vulnerability Taxonomy

KRISTEN BARTA* and CASSIDY PYLE*, University of Michigan School of Information, USA
NAZANIN ANDALIBI, University of Michigan School of Information, USA

Vulnerability intimately shapes the lived human experience and continues to gain attention in computer-supported cooperative work and human-computer interaction scholarship broadly, and in social media studies specifically. Social media comprise sociotechnical affordances that may uniquely shape lived experiences with vulnerability, rendering existing frameworks inadequate for comprehensive examinations of vulnerability as mediated on social media. Through interviews with social media users in the United States ($N = 20$) and drawing on feminist conceptualizations of vulnerability and social media disclosure and privacy scholarship, we propose a feminist taxonomy of social media vulnerability (FSMV). The FSMV taxonomy reflects vulnerability *sources*, *states*, and *valences*, within which we introduce the state of *networked vulnerability* and *ambivalent*, *desired*, and *undesired* valences. We describe how social media enable forms of vulnerability different from in-person settings, challenge framings that synonymize vulnerability with risk/harm, and facilitate interdisciplinary theory-building. Additionally, we discuss how *networked*, *ambivalent*, and *un/desired* vulnerability extend and diverge from prior work to create a theoretically rich taxonomy that is useful for future work on social media and vulnerability. Finally, we discuss implications for design related to granular control over profile, content, and privacy settings, as well as implications for platform accountability, as they pertain to social media vulnerability.

CCS Concepts: • **Human-centered computing → Empirical studies in HCI**.

Additional Key Words and Phrases: Vulnerability, identity, power, social media, taxonomy, feminist

ACM Reference Format:
Kristen Barta, Cassidy Pyle, and Nazanin Andalibi. 2023. Toward a Feminist Social Media Vulnerability Taxonomy. *Proc. ACM Hum.-Comput. Interact.* 7, CSCW1, Article 100 (April 2023), 36 pages. https://doi.org/10.1145/3579533

1 INTRODUCTION

> *"I define vulnerability as uncertainty, risk, and emotional exposure. To be human is to be in vulnerability." – Brené Brown*

Vulnerability is a fundamental condition of humanity, yet experiences of vulnerability can differ widely in implication and impact. For example, a person may feel vulnerable sharing intimate information about themselves with a new romantic partner. In addition, historically disenfranchised social groups may feel vulnerable to institutions, such as undocumented immigrants who may feel vulnerable in interactions with government officials. As vulnerability pervades diverse social contexts, common and scholarly definitions and characteristics abound. Often, vulnerability appears aligned with exposure to violence, risk of harm, and subjugation.

*Both authors contributed equally to this research.

Authors' addresses: Kristen Barta, krbarta@umich.edu; Cassidy Pyle, cpyle@umich.edu, University of Michigan School of Information, 105 S. State Street, Ann Arbor, Michigan, USA, 48104; Nazanin Andalibi, University of Michigan School of Information, 105 S. State Street, Ann Arbor, Michigan, USA, andalibi@umich.edu.

2573-0142/2023/4-ART100
https://doi.org/10.1145/3579533

Conceptualizations of vulnerability impact how scholars interpret and analyze vulnerability as well as how they engage in research or design with those whom they deem vulnerable. Scholarship in computer-supported cooperative work (CSCW) and human-computer interaction (HCI) explicitly and implicitly invoke vulnerability to describe individual and population-wide sensitive experiences with respect to technology use. There are numerous examples of CSCW and HCI papers and workshops designed to unpack the concept of vulnerability [10, 29, 55, 73, 74, 88] and provide guidance on conducting ethical research [10, 29, 73, 77] and design processes for and with "vulnerable populations" [29, 46, 55, 73, 106, 112]. For example, McDonald and Forte [74] argue for vulnerability, understood as susceptibility to privacy violations, as a useful concept for advancing online privacy theorization. However, workshops and papers in CSCW and HCI rarely explicitly define vulnerability. Implicitly, they invoke vulnerability as synonymous with a heightened potential to experience physical, emotional, or even financial harm [29, 46] or refer to entire populations as vulnerable, such as survivors of domestic abuse and immigrants [73].

We argue that while such conceptualizations of vulnerability are valid, they are partial in several ways. For one, framing vulnerability as synonymous with harm ignores understandings of vulnerability as potentially beneficial. The framing of vulnerability as harm thus limits our understanding of how individuals and social groups *perceive* and *experience* the totality of vulnerability online. Additionally, how researchers classify entire social groups as vulnerable is a critical question that motivates this study's investigation into how individuals *themselves* perceive and experience vulnerability in the context of their interactions with *and* on social media platforms.

Scholarship on constructs relevant to social computing, such as disclosure, privacy, and self-presentation begins to expand conceptualizations of vulnerability. Work on disclosure on social media suggests that being visible and sharing about oneself, particularly one's identity, on various platforms can carry both risks *and* benefits. For example, disclosing or making visible a stigmatized identity or experience can facilitate outcomes such as emotional support, social connection, and destigmatization [3, 9, 15, 45], as well as harassment, judgment, and relationship strain [5, 115]. The finding that beneficial outcomes, such as destigmatization, can extend *beyond* individuals and have social ramifications further complicates this tension [3, 15]. In combination, these areas of scholarship can be leveraged to position vulnerability (as it pertains to identity and self-presentation) as not only inclusive of but extending beyond harm, as well as carrying individual and social ramifications. Despite the insightful dialectical understandings of vulnerability found in disclosure, privacy, and self-presentation scholarship, CSCW and HCI scholarship lacks a systematic classification of vulnerability that accounts for vulnerability's complexity (*e.g.*, sources and compounding factors, such as marginality) in sociotechnical systems, such as social media. Moreover, while disclosure, privacy, and self-presentation scholarship considers risk and benefit in interpersonal interactions mediated by sociotechnical systems, these perspectives do not yet consider how people may experience risk and/or benefit in their interactions *with* these sociotechnical systems themselves.

Developing a more robust and nuanced understanding of perceptions of and experiences with vulnerability on social media is ontologically valuable. For one, it has the potential to directly shape how CSCW and HCI scholarship classifies, interacts with, and understands various individuals' and groups' interactions with *and* on social media platforms. Moreover, as social media platforms become ingrained into our lives as sources of entertainment, information, connection, and even income, it becomes necessary to contend with the ways sociotechnical environments may uniquely shape vulnerability across diverse individuals and social groups. As such, in this paper, we address the following central research question:

> *How do individuals perceive and experience vulnerability in their encounters with and on social media?*

While vulnerability has and will always exist in face-to-face settings, we focus specifically on what makes *social media* a unique context, including but not limited to opportunities for vulnerability across time and space, platform policies and practices, and algorithms that shape experiences on social media.

Given our interest in the ways identity informs social media vulnerability perceptions and experiences, we ground our understanding of vulnerability in scholarship on disclosure, privacy, and self-presentation within HCI, CSCW, and computer-mediated communication (CMC) fields. Moreover, feminist philosophy is a helpful lens for its attention to social positionality and identity as influential to vulnerability [93]. Thus, we draw from feminist philosophical frameworks [70] in tandem with social computing work to investigate the interplay between sociotechnical environments, identity, and vulnerability. Bridging these perspectives contributes to a unified framework of social media vulnerability, which in turn contributes to a more cohesive body of scholarship and advances theorization of vulnerability.

We propose a feminist taxonomy of social media vulnerability (FSMV), drawing from in-depth interviews with United States-based social media users. Aligned with arguments for studying social media experiences across platforms [117], we draw from individuals' experiences with vulnerability across their social media ecosystems. The FSMV taxonomy (1) extends extant taxonomic categories of vulnerability *sources* and *states* from feminist philosophy [70] to the social media context; (2) introduces the source of *sociotechnical* situational vulnerability as well as the state of *networked* vulnerability; and (3) contributes a new category of vulnerability: *valences*, inclusive of *ambivalent*[1], *desired*, and *undesired* vulnerability. Moreover, the FSMV taxonomy draws on recent scholarship explicating platform-perpetrated and -enabled harms [100] to consider platforms and algorithmic systems as *actors* bearing on vulnerability, as well as *contexts* that undergird vulnerability. The FSMV illustrates how perceptions of platforms, platform governance (*e.g.*, shadowbanning), and algorithmic outcomes (e.g., algorithmic symbolic annihilation [5]) may shape unique social media environments that exacerbate existing vulnerabilities and create new ones.

Through our analysis and taxonomy development, we contribute a definition of *social media vulnerability* as a condition of openness to affecting/being affected by other actors that is (1) perceived through networked interactions, (2) perpetrated or enabled by individual *and* sociotechnical actors (*i.e.*, users and platforms, including algorithms, affordances, and policies), (3) informed by factors including identity, social positionality, and stigma, and (4) may be perceived as un/desired or met with ambivalence by an individual.

We conclude by discussing possibilities for future CSCW and HCI research that invokes the FSMV taxonomy, including implications for researchers engaging with vulnerability and "vulnerable" populations in relation to social media. This taxonomy is attentive to both individual experience and perception as well as social positionality and sociotechnical actors, and it provides a unified lens through which to view identity visibility and self-presentation behaviors on social media across disciplines. In addition to implications for research, we draw from the FMSV to highlight considerations for design, related to more granular control over content visibility and consumption, profile visibility, and default privacy settings, as well as for platform governance.

2 LITERATURE REVIEW

We draw from feminist philosophy, CSCW, HCI, and CMC scholarship to review current understandings of vulnerability. Drawing from feminist philosophical work helps us understand how

[1]As we discuss, we draw on Gilson's [47] framing of vulnerability as ambivalent openness to affecting and being affected by others in face-to-face contexts to inform the valence category of social media vulnerability as ambivalent.

social identity and positionality interact with vulnerability perceptions and experiences. Additionally, CSCW, HCI, and CMC work informs how sociotechnical environments and affordances may uniquely shape vulnerability. Thus, we draw on visibility in social media, social computing, and HCI scholarship to bridge interpersonal processes and sociotechnical contexts and consider both in combination through the lens of vulnerability.

2.1 Vulnerability in Feminist Theory

Feminist philosophers have developed vocabulary around vulnerability to question who is disproportionately affected by and who bears responsibility for vulnerability. Broadly, feminist philosophy has tended to emphasize vulnerability's relationship to violence, weakness, and subjugation, though contemporary scholars have critiqued this association (see [102] for review). We draw on a feminist taxonomy of vulnerability, developed by Mackenzie et al. [70], as a context-sensitive framework against which to consider social media vulnerability [93].This taxonomy was developed in part to provide tools for context-sensitive analysis of vulnerability [93], and has been applied to this end [41], and in part to expand notions of vulnerability within research ethics [65].

Mackenzie et al.'s [70] taxonomy suggests that experiences of vulnerability, understood as susceptibility to harm, exist along *source* and *state* dimensions. *Sources* refers to the entities that give rise to an individual's experiences of vulnerability. The body, for instance, is an *inherent* source of vulnerability, while specific social, political, and economic contexts are *situational* sources of vulnerability. Finally, other humans give rise to vulnerability and are referred to as *pathogenic* sources. *States* include *dispositional* vulnerability, or vulnerability that is "not yet or not likely to become sources of harm" [70], as well as *occurrent* vulnerability, which refers to vulnerability that is enacted against an individual and which "require[s] immediate action to limit harm" [70]. Mackenzie et al. [70] provide the example that fertile people capable of giving birth are dispositionally vulnerable to complications in pregnancy and childbirth. Factors including access to medical care, physical health, and norms around childbirth inform whether this vulnerability becomes occurrent for a pregnant person.

This feminist philosophical taxonomy [70] has two significant strengths for the present project. First, it begins to challenge paternalistic assumptions of "vulnerable populations" by proposing inherent vulnerability, which acknowledges that all humans are vulnerable to some degree by virtue of our human needs (e.g., food, shelter, human connection). Second, it holds space for analysis via an identity and social positionality lens, as its framing of both sources and states acknowledges how various facets of the individual *and* the social worlds inform vulnerability.

Despite these strengths, Mackenzie et al.'s [70] taxonomy maintains an association between vulnerability and violence by conceptualizing vulnerability as facilitating harm. Other feminist philosophical works challenge the overdetermination of vulnerability as tied to harm. Gilson, for example, defines vulnerability in offline contexts generally as a "condition of openness to being affected and affecting" [47], and as such positions vulnerability as *ambivalent* and potentially affecting one in both positive and negative ways. Conceptualizing vulnerability as potentially enabling and limiting, she argues, challenges emphases on the avoidance of vulnerability and intimates the emancipatory potential of vulnerability when conceived of as openness or ambivalence [47]. Petherbridge [86] draws on Gilson [47] and similarly positions vulnerability as an "openness to the other" [86]. In so doing, Petherbridge [86] responds to criticisms that feminist perspectives equating vulnerability with violence perpetuate paternalism by aligning vulnerability with passivity and positioning "vulnerable" groups as lacking agency. Thus, these works argue that expanding vulnerability to a condition of "openness" to affecting and being affected by other actors creates room for additional conceptualizations of vulnerability, such as vulnerability as facilitating resistance [25, 102].

While a thorough review of vulnerability as resistance is beyond the scope of this paper, we note Butler's [25] recent work on vulnerability as influential in this tradition. Although Butler's earlier work that aligns vulnerability with violence has received criticism [86], her more recent work engages vulnerability "as a deliberate exposure to power" [25] and positions such vulnerability as deeply imbricated in political resistance. Schwartz [102] draws on a similar understanding in her analysis of selfies as a "reclaiming" of feminine vulnerability. This shift enables vulnerability to be considered as both exposure and precarity as well as agentic, marking an openness similar to that noted by Petherbridge [86] and Gilson [47].

Feminist framings of vulnerability thus maintain attention to the ways that social positionality and the human condition affect experiences of vulnerability, as well as how vulnerability may be leveraged to resist and challenge structures of power. In the following section, we review how CSCW and HCI scholarship has framed vulnerability, how theories of disclosure and privacy enable considerations of vulnerability as openness, and how an understanding of social media vulnerability grounded in feminist philosophy may similarly include vulnerability as resistance to power.

2.2 Vulnerability in CSCW and HCI

CSCW and HCI scholarship often frame vulnerability in terms of risk or harm, though work on online disclosure and interpersonal privacy in sociotechnical contexts implies that vulnerability may enable both risk/harm and reward/benefit. Scholarship on online disclosure, particularly stigmatized disclosure, further highlights how individual identity and social positionality influence perceived and experienced vulnerability, as well as how characteristics of online spaces facilitate outcomes of vulnerability. In this section, we briefly review these bodies of work to explore the possibility of a more inclusive understanding of vulnerability in CSCW and HCI. In highlighting attributes of social media that shape vulnerability, we also make space for an understanding of vulnerability that is explicitly grounded in a sociotechnical context.

2.2.1 Vulnerability as harm. Perspectives in social media, CSCW, and HCI scholarship tend to conceptualize vulnerability partially through the lenses of risk and harm. For instance, Pierce et al. [88] and McDonald and Forte [74] argue for centering vulnerability in understanding risks to online privacy and security and thus align vulnerability with the threat of harm. Recent typologies of online harm similarly suggest that the severity of harm experienced online is influenced by the target's vulnerability (or marginalization), further establishing linkages between vulnerability and harm [14]. Scheuerman et al. [98], for instance, position vulnerability as a dimension of online harm severity to capture the perception that harm against certain groups judged to be more vulnerable (e.g., children, animals) is more severe than against others deemed less vulnerable (*e.g.*, adults). Moreover, across countries, individuals perceive harms against "vulnerable groups" (*e.g.*, children) online to be particularly severe [59].

While these conceptualizations reiterate the link between vulnerability and harm, which we argue is a somewhat partial view of vulnerability, such framings are valuable in identifying the types of harm that may result from vulnerability on social media. Recent work addresses the potential for online environments to replicate the heightened vulnerability that marginalized folks experience offline through the concept of sociotechnical harms[2] [100]. In so doing, Schoenebeck & Blackwell [100] offer *platform-perpetrated* harms, or "those perpetrated by the design of platforms," and *platform-enabled* harms, "those facilitated by platforms but perpetrated by users or groups," as interrelated categories that identify platforms as actors and as contexts [100]. This differentiation aids in holding platforms accountable for harms incurred through policies and procedures such

[2]Sociotechnical harms are "online content or activity that inflicts psychological damage towards a person or community that compromises their ability to participate safely and equitably" [100].

as shadowbanning [11, 12], content moderation [44], and the amplification of distressing content [89]. Specifying platform-enabled harms highlights how platform architecture, including features, algorithms, and affordances, can enable interpersonal harm and amplify individual vulnerabilities.[3]

2.2.2 Vulnerability as risk and reward. Perspectives on self-presentation and disclosure, often used in CSCW and HCI scholarship, complicate associations between vulnerability and harm. Disclosure and privacy, two related research areas, implicitly invoke the concept of vulnerability through a dialectic approach that highlights tension between opposing but equally valid and possible outcomes. Dialectical disclosure theories, for example, center the tension between concealing and revealing information, as both are decisions informed by perceptions of disclosure risks (*e.g.*, security, stigma, face, relational, and role risks) and benefits (*e.g.*, self-expression, self-clarification, catharsis, relational closeness, and social support) [2, 17, 30, 35, 38, 80, 85, 87, 105].

Both disclosure and nondisclosure of personal information can mitigate and heighten vulnerability. Disclosure is apt at "reducing the risk that our interactions will be fraught with misunderstandings and failed expectations" [33]. For example, in the context of mental illness, disclosures can illustrate how mental illness affects daily life and facilitate understanding in interactions [43]. However, disclosure may also increase risks, such as rejection [33], harassment, or shaming [43], such that disclosure may increase perceived vulnerability. Conversely, nondisclosure can help people avoid potentially negative reactions to their disclosures, but may also foreclose opportunities for social support exchange [4]. Perspectives on disclosure and self-presentation thus implicitly align more closely with vulnerability as openness to affecting or being affected by others than vulnerability as solely harm.

Further, risk-reward perspectives underscore the connection between social positionality and vulnerability. A full review of social media scholarship on disclosure and marginality is beyond the scope of this article; however, marginalized communities and those whose identities are stigmatized [38] may experience heightened vulnerability in the form of risk and uncertainty [6, 15, 19, 51, 103]. For example, Andalibi & Forte [6] investigated the social media disclosure decision-making processes of women who experienced pregnancy loss, noting the ways in which the stigmatization associated with women who deviated from normative, linear narratives of motherhood placed women who decided to disclose their experience at risk of potentially psychologically damaging responses. Moreover, Pyle et al. [92] investigated similar decisions among LGBTQ+ folks who experienced pregnancy loss, noting how intersectional stigmatization of gender and sexual identity and the pregnancy loss experience influenced perceptions of risk and uncertainty during the disclosure decision-making process.

In summary, dialectical perspectives on disclosure and privacy aid in disentangling vulnerability from exclusively harmful or risky outcomes and reinforce an understanding of vulnerability as potentially enabling beneficial outcomes; these perspectives also suggest how social positionality informs perceptions of vulnerability. Although applications of these theories to online spaces have explored how affordances and features of social media impact perceptions of risk and benefit [6], it remains unclear how additional characteristics of social media more broadly (*e.g.*, algorithms) may also affect perceptions and experiences of vulnerability in these spaces.

[3]We ultimately draw on these categories in our analysis of how the sociotechnical contexts of social media informed participants' perceptions and experiences of vulnerability. As our emphasis is on delineating the influence of platforms as they relate to vulnerability (*i.e.*, as actor, context, and tool), rather than specific outcomes, we frame these categories in terms of vulnerability instead of harm. Doing so acknowledges the possibility that platforms may enable and deliver outcomes including and beyond harm, as well as allows us to precisely articulate how vulnerability on social media differs from vulnerability experiences in face-to-face contexts.

2.2.3 Vulnerability in sociotechnical contexts. In addition to vulnerability framed as enabling harm/risk and rewards/benefits, social computing scholarship has identified aspects of sociotechnical spaces that bear on vulnerability. Social media are, in part, defined by the potential for interactivity between users [27]. The perception of others (and their ostensible ability to interact with oneself) informs behavior on social media, including self-presentation, identity visibility, and privacy and disclosure decision-making [36, 42, 69, 71, 72, 84]. Interactions between individuals are implicitly associated with vulnerability through concepts such as pathogenic vulnerability [70] and platform-enabled harms [100], reviewed previously.

Social media also afford observation of others and their interactions on platforms [108]. This potential for observation can inform individuals' perceived vulnerability, and further shape behavior, as individuals seek to manage the vulnerability associated with being visible to others on a given platform. For example, Brock captures one form of observation in his concept of *weak-tie racism*, which describes "racism that is indirectly experienced through digital representation and the distribution, interactivity, or algorithmic repetition of antiblackness directed toward a specific Black body or bodies but abstracted through social media participation" [23]. In other words, weak-tie racism does not describe dyadic interactions in which one person is racist toward another, but rather exposure to racist content through one's network, others' interaction with content, and content delivery/organization algorithms. In this example, the Black body becomes a third-party observer and receiver of racist ideology and violence aggregated and distributed by platform structures. Moreover, social network sites have been described as "networked publics" [20, 110] and even "networked counterpublics" [57] whose socio-technical affordances (*e.g.*, persistence, replicability, scalability, and searchability) shape content consumption, production, and reception. The distinction between observation and direct experience may not be meaningful in the context of vulnerability in networked sociotechnical environments, as witnessing violence may similarly constitute harm as well as shape behavior and efforts to mitigate one's vulnerability in the future.

Observation of others afforded by social media platforms may also enable desired outcomes of vulnerability. For example, *network-level reciprocal disclosure* [6], in which encountering others' disclosures of stigmatized information spurs similar disclosures, can challenge and reduce social stigma [3, 15, 45]. Furthermore, scholars have argued that online spaces afford justice seeking for survivors of sexual violence [90, 96]. As such, the networked nature and observation afforded by social media may support beneficial social outcomes of vulnerability such as resistance and holding others accountable.

Additionally, characteristics of one's network, such as network size and composition, may inform perceived and experienced vulnerability [4, 24]. Buglass et al. [24], for instance, found that both larger and more diverse networks on Facebook positively correlated with vulnerability (understood as a "capacity to experience detriments" to one's well-being [24]). Beyond size and composition, the level of trust one has in a network provider and other network members may also inform perceived risks and vulnerability related to information visibility on a given platform [63]. The degree of control one perceives that they have over their own visibility further shapes vulnerability perceptions and is influential in where one chooses to be visible [18, 116] and how [4, 8, 21, 67, 109]. Thus, beliefs and perceptions about platforms, platform users, and platform-enabled control over information may further inform perceived vulnerability and explain why users perceive themselves as relatively more or less vulnerable on different platforms.

In combination, these works intimate a potential framing of vulnerability on social media as consisting of both risks/harms and rewards/benefits and as informed by individual positionality and sociotechnical context. Furthermore, these perspectives highlight perceived or observed and experienced vulnerability as facilitating individual or social outcomes. These conditions underscore the need to understand online vulnerability as grounded in a sociotechnical context. Bridging

these perspectives, as we do in this paper, contributes to a more comprehensive understanding of social media vulnerability in providing an organized means of understanding vulnerability as openness to affecting and being affected by others in sociotechnical spaces *as well as* the influence of sociotechnical spaces themselves (as context and actor) on perceived vulnerability.

3 METHODS

3.1 Recruitment & Interviews

We draw from semi-structured interviews with 20 U.S.-based social media users that addressed the topic of identity visibility on social media more broadly, including social media vulnerability. We recruited participants first through advertising the study on first author A's and the second author's social media accounts (generating 347 total engagements and 11,068 overall impressions). We then supplemented recruitment efforts using a research recruitment firm (which yielded 52 interested individuals, of whom 11 participated in interviews). Collaboration with the recruitment firm allowed us to target recruitment and draw from a more diverse pool of participants. Those interested in participating completed a screening questionnaire that, in addition to which platforms they used for personal use, asked respondents to self-identify (i.e., "please tell us about who you are") and describe how they identified on social media (*i.e.*, "please complete the sentence 'It is important for me to be seen by others as a/an... on my personal social media'"). We included these questions to allow individuals to use their preferred identity terminology and indicate the salience of their personal identities on social media; this was an important step given the centrality of perception to the study broadly. We also included optional, open-response demographic questions commonly used in participant recruitment (*e.g.*, sex, gender, etc.) [34] to contextualize respondents' online identity presentation. As demographic factors like gender, race, ethnicity, and education level may influence participants' experiences with online self-presentation and its resultant harms and benefits [60, 78], we included these optional questions. Participants had the option to disclose additional demographic information, and some did. However, we refrain from reporting them in Table 1 because not enough respondents chose to include this information. We received 127 combined responses to the survey and purposely sampled [83] participants to include a range of identities and identity intersections. We sought a range of racial and ethnic, sexual, gender, and physical and mental health-related identities to better understand how individuals who hold marginalized identities (1) perceive visibility and vulnerability on social media as informed by identity and (2) negotiate the visibility of their complex selves across their personal social media ecosystems. Saturation of observed themes [48] informed the final sample size of 20 participants, whose demographic information is listed in Table 1.

Interview questions explored participants' social media use, including platforms used, perceived audiences, self-presentation patterns, and networks. Additionally, the protocol covered participants' perceived vulnerabilities and risks associated with sharing on social media. Finally, interviews explored how participants perceived visibility on social media, including how visible (and by extension, vulnerable) they perceived their various identities (as described by them in the screening survey and interviews) to be on a range of platforms. Participants referenced numerous platforms in interviews, though most experiences appear connected to Facebook, Twitter, Instagram, Reddit, Tumblr, and YouTube. We specify platforms where relevant throughout our findings. First author A conducted interviews remotely in October 2020. Interview duration ranged from 60–110 minutes (avg. 81 minutes). All participants were offered $20 USD gift cards as compensation. The authors' institutional IRB determined the study exempt.

Table 1. List of Participants' Demographic Information

P#	Gender (pronouns)	Sexuality	Race	Ethnicity	Education
1	Man (he/him)	Gay	White/Native	Mexican	Graduate Degree
2	Woman (she/her)	White	Not spec.	Some Graduate	
3	Woman (she/her)	Queer	Asian	Indian	Graduate Degree
4	Man (he/him)	Straight	Asian	Indian	Graduate Degree
5	Man (he/him)	Queer	Asian	Hong Kong	Some Graduate
6	Woman (she/her)	Queer/Bisexual	White	Not spec.	Some Graduate
7	Woman (she/they)	Straight	Black	Slave Ancestry	Graduate Degree
8	Non-binary (they/them)	Queer/Bisexual/Asexual	White	European	Some Graduate
9	Woman (she/her)	Queer/Pansexual	Asian	Japanese/Okinawan	Graduate Degree
10	Woman (she/her)	Straight	Hispanic	Portuguese/Italian	College Degree
11	Non-binary (they/them)	Queer	Black	Not spec.	Some College
12	Woman (she/her)	Straight	Black	Not spec.	Some College
13	Woman (she/her)	Queer/Bisexual	Black	Not spec.	College Degree
14	Man (he/him)	Queer/Bisexual	Black	Not spec.	Some College
15	Man (he/him)	Not spec.	Black	Not spec.	College Degree
16	Man (he/him)	Gay	White/Hispanic	Not spec.	Graduate Degree
17	Non-binary/Genderfluid (they/them)	Not spec.	Brown	Mexican/Filipino	Some College
18	Woman (she/her)	Not spec.	Latino	Mexican American	College Degree
19	Woman (she/her)	Not spec.	Hispanic	Puerto Rican	Some College
20	Man (he/him)	Straight	Latino	Peruvian/French	Graduate Degree

3.2 Analysis & Taxonomy Development

We coded transcribed interviews using Dedoose, a qualitative coding software. As this paper is part of a larger project, first author A had already conducted descriptive coding [95] on the dataset; some of these categories (*e.g.*, experienced harassment on social media) informed the development of a vulnerability coding scheme. To develop this scheme, first author B reviewed all transcripts and wrote thematic memos that informed coding categories about vulnerability. Coding categories introduced in prior work on disclosure/privacy/support in online spaces influenced the thematic memos and the provisional coding they enabled. However, while drawing on provisional codes, first author B remained open to emergent themes, in accordance with open or first-cycle coding procedures [76]. All authors then met to discuss the inductively developed coding scheme several times. In doing so, we revised the scheme to eliminate redundant categories and incorporate emergent categories identified in memoing and coding checks. Before coding the entire dataset, the first authors co-coded three transcripts to check agreement and unitization between coders. Co-coding allowed the authors to identify points of disagreement and confusion in coding and resolve them through discussion. Co-coding three transcripts aligns with Campbell et al.'s [26] recommendation of assessing agreement using approximately 10% of a qualitative data set. As this was an exploratory study and we did not intend to quantify our codes, we determined that reaching intercoder agreement, rather than interrater reliability, was sufficiently rigorous [26, 75]. Once we reached agreement and finalized the coding scheme, the first authors collaboratively applied this coding scheme to the entire corpus. The final first-cycle coding scheme reflected inductive codes identified through memoing and coder agreement checks [76].

Following this first round of coding, the first authors used pattern coding to structure our data and identify connections across categories [76]. At this point, we compared our secondary coding categories to existing literature (*e.g.*, [70]) that identified sources and states of vulnerability and risk to develop the final categories of social media vulnerability which we introduce in the form of a taxonomy presented in this paper. Taxonomies provide means of classifying, organizing, and structuring knowledge of a concept or phenomenon [79]. In the context of information research, Nickerson et al. [79] note that taxonomies can be developed via an empirical-to-conceptual approach,

wherein the researcher(s) identify a "subset of objects that he/she wishes to classify," then identify a set of characteristics of the objects and group them into a conceptual taxonomy. Scholars can use interviews and qualitative analysis methods, such as the coding procedures described in our study, as part of the empirical-to-conceptual approach to taxonomy development. Qualitative methods are adept in facilitating sophisticated understandings of complex phenomena [1, 22, 111], such as vulnerability.

Nickerson et al. [79] posit that a useful taxonomy is concise, robust, comprehensive, extendible, and explanatory. We understand several of these attributes (*i.e.*, concision, robustness, comprehension, extendibility) as necessitating synthesis between inductively developed conceptual codes [22] and existing scholarship (*i.e.*, Mackenzie et al. [70]). Scholars such as Lewis et al. [68] have also used qualitative data from semi-structured focus groups to extend existing taxonomies. In drawing on extant scholarship to develop a concise, robust, comprehensive, and extendible taxonomy, we intentionally use the terminology introduced by these scholars. Doing so constitutes a form of citational justice [64], wherein feminist authors get recognition for their creation of foundational conceptual categories. We expand on how the FSMV reflects Nickerson et al.'s [79] attributes in *section 5.1*.

3.3 Limitations

We were intentional in recruiting a sample that represented a range of (multiply) marginalized identities, which may have surfaced particular experiences and perspectives on vulnerability as they relate to identity visibility on social media. That said, we did not require certain demographic information in our screening survey, such as participant age, income, and immigration status, which we acknowledge may bear on how participants perceive and engage with social media and vulnerability and visibility by extension. Rather, participants were asked to describe themselves, and if age, income, and immigration status were central to how they conceived of themselves, we expect that they would have included this information in the required survey responses. Aligned with best practices proposed by HCI researchers [58, 97] and our IRB, our screening survey only required demographic information critical for sampling needs and the research project. While we attend to the ways that identity (self-reported by participants) appears to inform participants' perceptions and experiences of vulnerability in our findings, given the exploratory nature of this work, we did not employ an intersectional analysis [99], which could elucidate further mechanisms of or additional taxonomic categories of vulnerability. Future research could assess and refine the FSMV taxonomy in connection with specific intersections of identities and/or experiences.

Additionally, while we acknowledge the importance of more globally dispersed samples (especially given the importance of social, economic, and political contexts on experiences with vulnerability), we intentionally recruited U.S.-based social media users to provide a more consistent context of identity-informed social positionality, power, and marginality. We invite researchers to explore to what extent our findings extend to or are challenged by contexts beyond the U.S.

Finally, additional research is required to test and validate the qualitatively derived, provisional FSMV taxonomy [79]. In validating the taxonomy, researchers may wish to use quantitative methods (e.g., surveys) that allow for larger and more diverse sample sizes to address the limitations of the present study.

4 FINDINGS

Although we did not code the data with a taxonomy in mind, we draw on Mackenzie et al.'s [70] feminist taxonomy of vulnerability for organizational clarity. We do so because this taxonomy's consideration of *sources* and *states* of vulnerability provides a valuable scaffold for understanding how social media vulnerability aligns with and departs from extant conceptualizations of "offline"

A person deciding to make their queer identity visible on their social media may perceive disclosure as potentially both risky and rewarding (*i.e.,* ambivalent); observing others' experiences disclosing queerness online (*i.e.,* networked) may shape perceptions of likely outcomes, such as judgment or harassment, from other people (*i.e.,* pathogenic), as well as perceptions of platforms (and associated features/affordances/algorithms) as contributing to vulnerability (*i.e.,* sociotechnical). Ultimately, the individual may perceive the vulnerability associated with queer identity visibility as personally beneficial (*i.e.,* desirable) or potentially detrimental (*i.e.,* undesirable). Should the individual make their queer identity visible, these vulnerabilities may or may not be personally experienced (*i.e.,* become occurrent).

Fig. 1. A vignette example of how an interaction on social media embodies intersecting dimensions of the FSMV taxonomy.

vulnerability. From Mackenzie et al. [70], our analysis reiterates *pathogenic* as a situational source of vulnerability and introduces *sociotechnical* sources to capture the ways that social media contexts lend additional considerations to these categories. *Inherent* vulnerability (*e.g.*, corporeal vulnerabilities) did not surface as salient in our data, and thus we do not include it in the FMSV. We further introduce a *networked* state of vulnerability, which we argue more fully captures the effects of observed vulnerability afforded by sociotechnical contexts on vulnerability perceptions. Finally, to capture the risk-reward tension inherent in information revelation (*e.g.*, as implied in disclosure and privacy perspectives, reviewed previously), we propose *valence* as a category that comprises *undesired*, *ambivalent*, and *desired* forms of vulnerability, as perceived by individuals. We reiterate that, as in Mackenzie et al.'s [70] taxonomy, categories of the FSMV taxonomy intersect. Thus, the presented examples in our findings may illustrate multiple taxonomic categories. To articulate this point before providing detailed findings, we offer a vignette example in Figure 1. Participant examples included throughout our findings further illustrate intersections of these categories.

4.1 Social Media Vulnerability Sources

We identify *situational* sources of social media vulnerability. Specifically, we (1) introduce *sociotechnical* vulnerability as a specific form of situational vulnerability, and (2) extend Mackenzie's *pathogenic* vulnerability in in-person settings [70] to identify *pathogenic* vulnerability as a subset of social media situational vulnerability. In doing so, we consider how the sociotechnical context of social media intersects with vulnerability and identify platforms as both enabling and perpetrating vulnerability. Additionally, we address interpersonal sources of pathogenic vulnerability, such as fellow social media users.

4.1.1 Sociotechnical situational vulnerability. While Mackenzie et al.'s [70] feminist philosophical taxonomy of vulnerability incorporates a broad situational category, encompassing social, political, economic, and environmental situations that may promote vulnerability, we argue that a FSMV taxonomy must contend more explicitly with sociotechnical situations that can cause and/or exacerbate vulnerability. We thus introduce the sociotechnical category as a subset of the situational source of vulnerability.

Informed by Schoenebeck and Blackwell's [100] descriptions of social media harms, we invoke the sociotechnical category to understand how vulnerabilities are "platform-enabled" and/or "platform-perpetrated." In keeping with Schoenebeck and Blackwell [100], we note that the boundary between these categories is imprecise and that individuals' experiences with vulnerability online can be at once platform-enabled and platform-perpetrated. However, both categories indicate that platforms are sources of vulnerability as contexts or actors.

Platform-enabled vulnerability. Participants often perceived *platform-enabled vulnerability* in experiences that were facilitated by technical features of a social media platform. Several participants

Dimension	Category	Definition
Source	Sociotechnical*	A form of situational vulnerability [70] that explicitly considers sociotechnical contexts; includes platform- enabled and platform-perpetrated vulnerabilities (informed by [100]'s harm categories). We use the term sociotechnical to encompass the ways platform features, policies, and social contexts affect perceived vulnerability, as evident in our data.
	Pathogenic	A form of situational vulnerability introduced in feminist philosophy [70] and extended to the social media context in which an individual's actions bear on perceived vulnerability
State	Networked Vulnerability*	A state in which one's vulnerability is informed by and/or contributes to another's; networked vulnerability blurs distinctions between dispositional and occurrent vulnerability [70].
	Occurrent Vulnerability	A state of vulnerability introduced in feminist philosophy [70] and extended to the social media context that requires immediate action to manage or alleviate; direct experiences of vulnerability arising from interactions with person(s) or platform(s).
Valence*	Undesired*	A valence of vulnerability introduced in the social media context; vulnerability that one is unwilling to assume or perceives as more likely to facilitate harm to oneself or others than benefit.
	Ambivalent	A valence of vulnerability introduced in feminist philosophy [47] and extended to the social media context; vulnerability that is inherent to a space and potentially facilitates both benefits and harms.
	Desired*	A valence of vulnerability introduced in the social media context; vulnerability that one is willing to assume or perceives as more likely to benefit oneself or others than harm.

Table 2. Feminist Social Media Vulnerability (FSMV) Taxonomy, including source, state, and valence. Some categories observed in our analysis draw from past work in in-person [47, 70] and social media [23, 100] settings. Others (indicated by *) are new categories we discovered through our analysis.

remarked that Facebook, where individuals typically must accept each other as "Friends" to engage with each other, contrasted with Twitter, which enables unreciprocated engagement and interaction with users not in one's network. While participants described feeling vulnerable both on Facebook and Twitter, network composition and connection mechanisms intimately shaped their perceptions of vulnerability. When explaining why he opted for a Bitmoji Twitter profile picture, as opposed to one of his face, P5 (man, queer, Asian/Hong Kong) replied:

> Because of the democratized nature and publicness of Twitter, I didn't like that very remote strangers can see my face. Because you know, Facebook is naturally private, you have to accept friend requests to have people see most of your things. [...] but Twitter is not that way.

This excerpt illustrates how the network structure of Twitter that allows for greater engagement from weak or latent ties plays a role in shaping possibilities for social interactions on Twitter and catalyzing perceptions of vulnerability. Here, it may not be that P5's face being visible necessarily incurs outcomes of vulnerability, such as harassment, but rather that P5 perceives the openness of Twitter (*i.e.*, openness to being affected by others) as contributing to vulnerability. P5's recall of an experience tweeting about YouTube personality PewDiePie (who has been critiqued for anti-Semitic remarks and white supremacist messaging [94]) further illustrates a possible consequence of this openness. He explained:

> I tweeted something about him not wanting to explicitly apologize to the Jewish community. [...] I tweeted that, and perhaps people found my tweet through keywords. I didn't hashtag anything, but I did write his name on a tweet. And so, a few fans of his from his fandom came after me. And they're like, 'You don't know him at all.' Like, 'he said multiple times that he didn't intend to target any community of people,' things

> like that. So, it was really quick. The response was swift, like within five minutes of me tweeting that I got three really defensive responses from his fandom. And I was like, 'Oh, okay, well, I don't like that at all.' [...] so, I deleted that tweet really soon after.

In this example, P5 identifies hashtags and keywords as features that, because of the searchability afforded by Twitter's structure, potentially bear on perceptions and experiences of vulnerability. In this way, Twitter's structure may *enable* vulnerability by surfacing this tweet in search results and allowing non-networked users to directly comment on or otherwise interact with P5. In response to this experience, P5 reported deleting the tweet, which, in the context of this example, effectively stifles discussion of an influential (and white, male) media figure and their actions toward a historically discriminated-against population.

Platform-perpetrated vulnerability. Several participants' perceptions of vulnerability centered around platform governance, specifically the phenomenon of shadowbanning [4]. For users who embody historically marginalized identities, the perception that platforms like Instagram are removing or rendering invisible content disproportionately created by marginalized users (irrespective of whether this occurs) can directly impact perceptions of their own vulnerability. Participants shared the perception, for instance, that shadowbanning disproportionately affected users who held marginalized identities or advocated for marginalized users. P1 (man, gay, White/Native/Mexican), for instance, referenced *"some of the platforms having shadow bans on certain hashtags or things for visibility, like on the Black Lives Matter movement or on trans rights,"* while P19 (woman, Hispanic/Puerto Rican) referenced *"this big thing where there was shadowbanning [of] people who are talking about LGBT rights."* Many of our participants observed or had heard of shadowbanning and believed that shadowbanning disproportionately affected marginalized communities but had not personally experienced it. That said, P11 (non-binary, queer, Black) commented on Twitter's policies and account-locking practices concerning Black users' expressions. They explained:

> Twitter is especially confusing, because if two Black people are tweeting back and forth on Twitter, and they're using the N word, clearly, it's not a hate group, you know, because some Black people use the N word like that, they use it as like a term of endearment, whatever. But Twitter sees that and they're like, 'You cannot use racial slurs, you are banned for a week,' you know, because the algorithm doesn't have the time to sit there and be like, is this person white and saying this word or are they you know, Black? It's weird.

While the practice of automatically moderating the use of racial slurs on a platform may address specific forms of harm, P11 described the algorithm's lack of discretion in flagging and acting on certain terms, which may contribute to further silencing and policing of marginalized communities over language that is culturally situated and contextual.

Beliefs about platform practices can also promote vulnerability that affects marginalized folks' abilities to make a living, particularly when their jobs are heavily reliant on creating and maintaining a social media presence. For example, marginalized artists and sex workers who rely on the platform for attaining financial resources bear vulnerability when they experience the effects of shadowbanning or other forms of content suppression by prominent platforms, notably Instagram and TikTok. P6 (woman, bisexual, White) recounts: *"if somebody mentions OnlyFans on TikTok, like that stuff gets taken down. And so it's like, well, that's directly impacting people's income and their work by making them invisible."* These examples demonstrate users' perceptions of platform policies around moderation as potentially increasing the vulnerability of marginalized communities and creators, who rely on platforms for social support and professional success. Perceptions of

[4] Shadowbanning describes a platform's actions "which dramatically reduces posts' visibility by hiding them from its Explore page without warning" [12].

shadowbanning and other forms of content moderation/suppression thus offer an illustration of platform-perpetrated vulnerability that emanates from the complex and often opaque relationship between platform design (*i.e.*, the development of news feed algorithms) and platform governance (*i.e.*, algorithms used to auto-flag and auto-remove content).

In sum, sociotechnical environments propagated by social media platforms can create and contribute to vulnerability, either by exacerbating vulnerability or directly imposing vulnerability on users. Although we challenge framings that align vulnerability only with harm, we note that our participants did not explicitly associate platforms *as actors* with beneficial outcomes of vulnerability. Elsewhere (*e.g.*, 4.2.1 and 4.3.3), we note instances in which platforms *as context* appear to enable beneficial and desirable outcomes to vulnerability.

4.1.2 Pathogenic Vulnerability. Pathogenic vulnerability, drawn from Mackenzie et al.'s [70] taxonomy stems from the (mis)understandings, judgments, and reactions of others, and is informed by social positionalities. As introduced in *section 4.1.1*, social media platforms may enable pathogenic vulnerabilities but do not enact them, per se. Rather, other users ultimately enact pathogenic vulnerability. Often, participants perceived pathogenic vulnerability as dispositional (*i.e.*, observed or anticipated) rather than directly experienced. Participants such as P3 (woman, queer, Asian/Indian), for instance, acknowledged vulnerability associated with her sexual identity:

> The way I identify myself as queer is by being a queer ally. [...] It's kind of how I present myself. And that definitely has to do with the fact that I know many of the people who follow me are from when I grew up in India, and I don't actually know how they feel about sexuality in general, and I kind of don't want to find out.

P3 thus describes vulnerability to judgment and other undesired reactions as informing her self-presentation on social media. Notably, the vulnerability P3 associated with their sexual identity being visible resulted in P3 presenting an identity she perceived as related to her authentic identity, but less vulnerable.

Many participants' fears regarding pathogenic vulnerability concern social media content being visible to employers (present or future; akin to imagined surveillance, monitoring that could occur and bring about future risk/opportunity, as described by [39]), and as such touch on context collapse [71] and affordances like content persistence, searchability, and association [107]. P15 (man, Black) spoke to a general vulnerability bearing on employment and other opportunities:

> "Just the way that the internet works now, where if you have something in your past and you posted it on Twitter, or something, or on Facebook and then, say you get a big-time job or something, and now people are looking for holes to poke through and they find some sort of posts there. And then that can have repercussions on your whole entire life, you wouldn't know. It might've been something in the past or something that you maybe forgot about. So, I think that's a bigger part of why I don't use my identity."

While P15 had not encountered this personally on Twitter, they reported similar experiences "in real life" and observed repercussions for others on Twitter as informing their preference for anonymity on Twitter. Pathogenic vulnerability, stemming from interpersonal interactions, can affect myriad identity domains, including sexual and professional identities, as these examples demonstrate.

Participants' perceptions of pathogenic social media vulnerability also extend to platform perceptions more broadly and further illustrate how platforms may enable pathogenic vulnerability. That is, some participants referenced specific platforms' reputations as informing their identity and personal information visibility. For instance, P11 (non-binary, queer, Black) enjoyed Reddit,

but used the space anonymously due to their belief that, because posting and activity histories are available to other users, *"Reddit [users] hold you way more accountable" for one's content than users on other platforms"*. They explained:

> On Reddit, I don't even get into details about where I live, because people are crazy. And they will be like, 'she posted at exactly this time, and she posted a picture, and tracing back to her IP she lives here'.

Regarding Twitter, P14 (man, bisexual, Black) noted, "*I have no issue having a normal or respectable debate, but a lot of times that's not what people are trying to do on Twitter. Some people have been doxxed on Twitter, so it's those kind of scenarios [I don't want].*" As a result of this perception, P14 reported sometimes feeling unsafe posting about his political and sexual identities on Twitter. These examples center other social media users as perpetrators of harm (i.e., doxxing), but also show how perceptions of platform context, including userbase, may inform perceived vulnerability. Moreover, these examples allude to the ways that platform-enabled vulnerabilities may span both sociotechnical situational and pathogenic sources of vulnerability.

In identifying sociotechnicality and pathogenic sources of vulnerability, the FSMV taxonomy both delineates between platforms and social media users as perpetrators of vulnerability, as well as platforms as enablers of vulnerability. As our examples show, social media vulnerability sources may act independently or in concert to inform perceived as well as experienced vulnerability.

4.2 Social Media Vulnerability States

Our analysis yielded two social media vulnerability states: *networked* and *occurrent*. The former is a novel vulnerability state that we contribute, and the latter originated in in-person vulnerability literature but is analyzed here as a vulnerability state that is equally relevant to sociotechnical contexts [70].

4.2.1 Networked Vulnerability. Given the imbrication of vulnerability and visibility, sociotechnical contexts can affect perceptions of vulnerability. As noted, concepts such as weak-tie racism [23] address how social media connectivity can result in vicarious trauma and other consequences for marginalized groups. Participants similarly suggested that association (i.e., connections to other users; [107]) could increase their own perceived vulnerability to harassment or judgment, with implications for networked others' vulnerability. Conversely, observation of others' experiences of vulnerability informed one's own perceived vulnerability. We introduce and position *networked vulnerability* as a state, rather than a source, of vulnerability to bring observed or vicarious vulnerability [23] into conversation with occurrent or directly-experienced vulnerability [70]. Networked vulnerability, we argue, captures the perpetual state of awareness, preparation, and mitigation of vulnerability on social media.

When asked about unwanted experiences on social media, many participants reported that, although they had not personally experienced harassment or similar consequences, their observations of the platform(s) and other users informed their own visibility choices, and thus perceptions of vulnerability. As alluded to in connection with platform-enabled vulnerability, participants assessed their own vulnerability through observing collective attitudes and behaviors. P17 (nonbinary/genderfluid, "brown"/Mexican/Filipino), for example, described how observing misogyny on Reddit informed their own perceptions of vulnerability associated with gender identity visibility:

> There was a subreddit, you know, pardon my language if this is too explicit, but it was called 'pussy pass,' [...] dedicated to posting videos of women that were acting out in some way, maybe yelling in a man's face, or even hitting him, and the man replying by beating the shit out of her, essentially. That was really, that was on the front page consistently for a while and that would get like, you know, thousands, tens

> of thousands of likes. And it made me very uncomfortable. It definitely reminded me that, in these other posts of like, cute dog pictures and relationship stories, like, the very big part of Reddit that actively uses Reddit every day does not like women.

Consequent to these observations, P17 reported a general practice of not disclosing their gender identity (*e.g.*, non-binary/genderfluid) on Reddit. The sense that one does not belong or is not respected due to their gender identity, informed by observing others in networked online spaces, thus affected P17's perceived vulnerability, even though discrete interactions with individual users elsewhere on Reddit had not resulted in harm. This example also highlights how networked vulnerability extends dispositional and occurrent vulnerability. As a person with a marginalized gender identity, P17 may be at greater dispositional risk for harassment than persons without [40, 91]. Observing attitudes toward and treatment of women by Reddit users surfaces this disposition and results in P17 taking steps to mitigate their vulnerability, as they might in cases of occurrent vulnerability.

In other cases, participants assessed their own vulnerability by observing antagonistic behavior directed at particular users rather than discrete identities. As P15 (man, Black) explained, *"it just seems like every month, someone does something on Twitter that they shouldn't have...and it's just learning from other people's experience. You just don't want to put yourself in that position."* Similarly, P7 (woman, straight, Black) noted, *"when I see how [others] react to other posts, that definitely has impacted what I decide to post. Because some people just don't have, like, any respect for other people. So I've chosen not to do certain things."* P7 specified a concern that others could take her posts out of context, which would cause issues in her personal life. These examples suggest that networked vulnerability may be informed through observations of actions taken against targeted individuals and attitudes toward particular identities or ideologies, even when targets are not explicitly known or networked others (*i.e.*, friends, followed accounts).

In addition to observing others' experiences of networked vulnerability and associated consequences, participants implied that others in their network might become vulnerable through association and often actively took precautions to manage this vulnerability. Specifically, the fear that networked vulnerability could affect interpersonal and professional relationships appeared to inform perceptions of networked vulnerability and related management strategies. This phenomenon appeared especially salient in connection to sexual identity visibility. P13 (woman, bisexual, Black), for example, explained:

> I mentioned that I'm polyamorous and I have two partners, and one of my partners, even though he's on Facebook, we're not Facebook friends. Which, you know, kind of bugs me a little bit. But at the same time, I understand because, I mean, the majority of his Facebook friends are family or co-workers...or friends. So, he just isn't comfortable being very visible.

In this case, the visibility of P13 as not only polyamorous—an often stigmatized identity [104]—but also connected to her partner could compromise her partner's privacy boundaries, cause speculation, and potentially make her partner vulnerable to judgment, harassment, or loss of opportunity via context collapse [71]. P13 and her partner managed this perceived vulnerability by not being formally connected on Facebook. Similarly, P16 (man, gay, White/Hispanic) noted precautions taken to manage networked vulnerability that could affect his partner. He explained:

> My boyfriend is one of the few people in America who's not on Facebook. And so, I will post pictures of us, [but] I will not post his name. He works for a school district, which does, they do have non-discrimination protections for LGBTQ people, but he works...as an administrator. And I don't want to cause any problems for, you know, a parent finding out stuff and making his life "more difficult than it needs to be."

In this example, P16 points to his boyfriend's professional identity as an administrator as potentially intersecting with and exacerbating vulnerability informed by homophobia in the workplace. In addition to institutional protections (*e.g.*, district non-discrimination policies), P16 reports taking additional precautions, such as not mentioning his boyfriend's name on social media, to further manage the perceived networked vulnerability associated with sexual identity.

In combination, these examples show that tactics used to manage one's visibility, such as not friending or tagging significant others, may also be used to manage others' vulnerability. These tactics echo similar strategies noted in extant work (*e.g.*, [8, 49, 67]). The awareness of one's vulnerability as informing another's, and the strategic management thereof, points to space for individual agency and action in the face of vulnerability. In doing so, it challenges assumptions that exclusively align vulnerability with weakness and victimhood.

Indeed, in some cases, the strategic management of sexual identity visibility created space for desired connections and further aided in managing networked vulnerability. For example, P1, who identifies as a gay man, described the experience of posting about traveling to Oman and interacting with other gay individuals online. He explained:

> I'll get someone being like, 'Oh yeah, and I'm gay too,' and I'm like, 'Oh, so I guess like the algorithm worked to show them my post or whatever'...those people might be uncomfortable following someone that is a very visible...gay influencer who likes to travel, but they're not really going to get in trouble for following someone like me, who's much less visible [...] If you went on my page, it wouldn't be bombarded with gay flags, right? So, they might feel more comfortable because of that. So, there might actually be, like, a conversation that takes place.

In this example, the relative visibility of P1 as a user on Instagram, as well as the relative (in)visibility of P1's gay identity on the platform, manage the networked vulnerability that stems from being associated with gay social media users while living in a country that criminalizes homosexuality. P9 (woman, pansexual, Asian/Japanese/Okinawan) noted a similar instance in which the visibility of her same-gender relationship facilitated connection. She explained:

> When I was dating [woman's name], there was at least one person who would, like, direct message me comments to something I posted or questions to something I posted. And he has never said this to me in so many words, but I suspect it's because his family is extremely conservative. And he came out as gay. He actually never came out as gay to his family, but to me he did. And because we had mutual friends, including his brother—and I don't know if his brother is homophobic—he would engage with me in a way that was still protecting his identity.

In this case, P9's friend appears to leverage the relative invisibility of communication channels, particularly direct or private messages as compared to public comments, to manage networked vulnerability that may be otherwise heightened due to mutual or reciprocated connections. Thus, while in many cases networked vulnerability appears associated with undesirable outcomes (*e.g.*, P13, P16), the experiences of P1 and P9 suggest that strategic management of identity and communication visibility may mitigate some degree of harm and enable desirable outcomes, such as connection with similar others. As we discuss further in *section 4.3.3*, this form of desired vulnerability may undergird processes such as destigmatization that challenge hegemonic power relations and illustrate vulnerability as resistance.

Networked vulnerability as a state of vulnerability further highlights how the sociotechnical context of social media, including affordances such as visibility and association, may enable and manage pathogenic vulnerability and how social media blurs distinctions between dispositional and occurrent vulnerability. That said, we distinguish between networked and occurrent vulnerability

to acknowledge the unique situation of directly experiencing undesired outcomes to vulnerability, in addition to observed, vicarious, and anticipated experiences of vulnerability. We do not attempt to infer their respective magnitude or severity in reporting this distinction. Rather, we acknowledge sociotechnical environments' unique influence on experiences of vulnerability. We do so with full acknowledgment that we cannot speak to the comparative magnitude or severity of outcomes across these categories in this study, nor do we suggest that would be a fruitful line of inquiry.

4.2.2 Occurrent Vulnerability. While infrequent, some participants described occurrent states of vulnerability wherein they directly experienced the enactment of vulnerability via social media platforms. Typically, participants referenced occurrent and pathogenic vulnerabilities in the form of harms perpetrated by other users. Sometimes, as noted by P2 (woman, bisexual, White), participants experienced firsthand vulnerability in response to strangers on social media. P2 recounted an incident in response to a post that expressed her feminist identity:

> I had a random dude find my account. I don't know him. He doesn't follow me. But he reported my post because I said something along the lines of 'men are trash.' And he was like, 'That's fucking discriminatory.' And I was like, 'You don't know what systemic misogyny is like, you don't really know anything about feminism. So please fuck off.' And he reported me and so that post was taken down.

P2 later explained, *"That guy was specifically looking for that, and I could tell because I didn't know him. So, he must have looked at specific hashtags."* This excerpt highlights the vulnerability that can arise from hostile interactions with other social media users and how affordances (*e.g.*, keyword searchability) and governance (*e.g.*, content moderation and removal systems) potentially contribute to platform-enabled vulnerability. This example further highlights, in addition to perceptions of shadowbanning related earlier in this paper, that invisibility and silencing are outcomes of social media vulnerability. Experiences such as P2's can inform perceptions of danger or trouble that influence how individuals engage with platforms. Interactions that result in content deletion or non-disclosure practices can, by extension, compromise individuals' ability to access benefits, such as social support, through platforms.

Based on what we observed from our participants, occurrent vulnerability on social media is often interpersonal. It may intersect with pathogenic sources to inform one's overall experience of vulnerability. Moreover, the sociotechnical aspects of social media can exacerbate this interpersonal or pathogenic source of vulnerability, which may result in relational turbulence and relationship dissolution.

Additionally, in considering vulnerability beyond solely risk and/or harm, we address how occurrent vulnerability aligns with Gilson's [47] definition of vulnerability as openness. Some participants, for instance, recalled how they strategically enacted vulnerability in curated safe spaces to access mostly intangible resources like social support from supportive others. P2, for example, noted, *"I haven't really dealt with a lot of difficulties because I've made sure that Instagram is more of a safer space for me to just do whatever the fuck I want."* While unclear whether the man who reported her "men are trash" post influenced her decision to carefully curate Instagram as a safe space, P2 did, in fact, work to separate audiences and ensure that followers of her private account, where P2 posted "kinky" content, had consented to be there. P2 continued:

> The kinky account is specific. So, like that one I made specifically to share that kind of vulnerability, right? [...], I've been trying to use that as a practice for myself of like, it is not shameful to be sexual and all these things and it's not shameful to have kinks and the specific things I have, and I'm sharing those things as a practice. [...] I don't want to just post that without someone's consent. [...] I tell people, 'I have this account, if

> you would like to follow it, it is specifically this content. If you would like to follow it, you can.' But I don't like to post stuff like that on my personal [account] because I don't want to just, if people don't want to see me in a sexual way, I don't want to just bombard them with it.

In considering and enforcing consent via privacy settings, P2 created a "safer space" to explore her sexual identity, affording her desired occurrent vulnerability while managing undesirable occurrent vulnerability for her followers. Similarly, P8 (non-binary, queer, White) described Tumblr as a place where "I can be totally myself," as they had been on the site for ten or more years and had cultivated a community of mutual followers. They continued:

> I feel like I show a lot more of myself on Tumblr. I feel like I am, yeah, I would say more honest, because I feel like I'm less worried about people judging me [...] Even though I don't know everyone who follows me on Tumblr, it still feels a little bit like it's an insular community, like everybody knows me.

As a result of long-term involvement and gradual community development, P8 cultivated a space in which occurrent vulnerability appears associated with authentic self-expression and connection. We thus find that participants highlighted how occurrent vulnerability reflected both vulnerability as risk and vulnerability as openness, aligning with valences of vulnerability as un/desired, which we highlight in the next section. Whether vulnerability is perceived as un/desired and whether individuals feel they have control over their vulnerability carry implications for how vulnerability bears on power. As we discuss in *section 4.3.3*, vulnerability that is desired and enacted by individuals potentially resembles vulnerability as resistance to power and hegemony.

In reflecting upon the various states of vulnerability outlined in this section, we reiterate that states are, to some extent, temporally bound. Over time, vulnerabilities from various sources can move from networked to occurrent as individuals encounter new situational factors. However, states of vulnerability are also bound to identity and power. While vulnerability exists amongst people of all identities, those possessing historically marginalized identities experience more direct (*i.e.*, occurrent) and indirect (*i.e.*, networked) violence and harassment online [11, 37, 66], supported by our findings, and reflected in characteristics of dispositional vulnerability [70]. Thus, an examination of social media vulnerability that derives itself from feminist philosophical work must equally engage with the ways identities and power structures work in tandem to inform taxonomic categories. Our findings highlight instances in which participants' identities inform perceived (*e.g.*, P17 and gender identity) and experienced (*e.g.*, P2 and political identity) vulnerabilities, and we expand on this discussion in *section 5*.

4.3 Social Media Vulnerability Valences

We introduce valences as a taxonomic category and dimension of vulnerability to explicitly divorce conceptualizations of vulnerability from solely violence and harm. That is, in addition to recognizing vulnerability as potentially resulting in harm, we acknowledge vulnerability as potentially resulting in beneficial outcomes. As such, we draw on Gilson's [47] framing of vulnerability broadly as "openness to affecting and being affected" to inform the valence of ambivalent vulnerability on social media. Moreover, we introduce the terms *desired* and *undesired*, rather than *positive* and *negative* associations, to further ground vulnerability in individual perception, as what may be desired for one individual may be undesired for another. Further, this terminology better captures vulnerability as both dispositional (*i.e.*, anticipated but not yet realized) and occurrent (*i.e.*, realized) than positive and negative, which we argue emphasizes realized outcomes. This un/desired terminology thus: (1) affords a more nuanced understanding of how perceived vulnerability affects behavior and visibility choices on social media (*e.g.*, what, where, and to whom one chooses to be visible),

and (2) resists paternalistic determination of vulnerability/outcomes as unilaterally positive or negative. While conceptualizations of vulnerability as harm are important in that they help us think about sociopolitical injustices and how they disproportionately impact those who are historically marginalized, we argue that conceptualizations of vulnerability as desired are equally important.

4.3.1 Undesired Vulnerability. In discussing their own identity visibility on social media, participants alluded to undesired vulnerability associated with being present on social media generally and audience concerns (*e.g.*, context collapse, lack of control over visibility) enabled by platforms. As such, undesired vulnerability intersects with sociotechnical and pathogenic vulnerability sources. Indeed, many of the previously related examples illustrate undesired vulnerability, as evident in mentions of management strategies, such as withholding information via non-disclosure and deleting content or having content removed.

Some participants noted that vulnerability appeared unavoidable on social media (which we expand on in the following section) and perceived this vulnerability as undesirable. For instance, P5 (man, queer, Asian/Hong Kong) discussed observing accounts they followed on Twitter. In noting that both very active and less active (in terms of posting activity) accounts appeared susceptible to harassment, P5 commented, *"it's an interesting thing to think about, because you don't have to have a strong presence to be attacked by people, you just kind of have to be there at all, to be attacked or harassed."* As a result, P5 withheld certain personal information from social media that might be considered mundane in other contexts, such as a photo of his face. He further explained:

> I mean, it's one thing to walk on the street and have people look at your face. But it's a different thing to be on the internet with all of your opinions and comments and thoughts published, in a way, and then matching that with your actual biological face and appearance.

P5 thus alludes to the combination of available information as affecting his visibility and associated vulnerability. He manages this perceived vulnerability by withholding choice information, such as his physical appearance. Other participants similarly alluded to the visibility of certain information contributing to their discomfort. P3, for example, connected her discomfort with visibility to audience perceptions on Twitter. P3 (woman, queer, Asian/Indian) explained:

> I don't think I want to put myself in a position where I'm vulnerable [on Twitter]. [...] I think that because I don't know who is looking at my Twitter, I think, a lot. So, I almost don't allow myself to be vulnerable because I don't know who's going to see me being vulnerable.

Here P3 alludes to the composition of their network, and awareness thereof, as informing their perceptions of vulnerability and associated outcomes as undesirable, similar to Buglass et al.'s [24] findings. Together, these examples suggest that, in the absence of a clear motivation or target audience, the vulnerability associated with being visible on social media may be perceived as undesirable and/or as more likely facilitating undesired outcomes than desired. While constraining one's own visibility online as a means of managing vulnerability is not necessarily troubling on its own, this self-silencing takes on additional significance when contextualized by participants' perceptions of vulnerability as unpredictable, undesirable, and, as previously discussed, disproportionately affecting marginalized groups.

4.3.2 Ambivalent Vulnerability. In opening space to consider desired vulnerability, in addition to undesired vulnerability that prior work traditionally considered, it becomes necessary to invoke a third category that recognizes that individuals do not always perceive vulnerability as desired or undesired. Indeed, the risk-reward tension central to processes like disclosure, in which disclosure is vulnerable but is neither harmful nor helpful until a response or outcome is achieved, implies the

presence of this third category. Moreover, feminist philosophical work [47] implicitly articulates ambivalence in positioning vulnerability as openness to affecting and being affected by others. In our framing, and based on our findings, un/desired determinations may be separate from considerations of outcomes and instead be informed by personal preference (*e.g.*, individual attitudes about what personal information is private and/or appropriate to share on social media). Thus, vulnerability as ambivalent captures the perspective espoused by some of our participants that vulnerability just is and is assumed to be part of any social media experience, extending notions of ambivalent vulnerability to social media contexts. For instance, some participants remarked that *"being visible is vulnerable"* (P2) and accepted this without attributing a more specific valence to it. Similarly, P7 (woman, straight, Black) noted:

> I'm being vulnerable sharing anything that's personal. Because you don't really have privacy on anything. Anything that you share can be shared to anybody. So, I think there's vulnerability everywhere.

In stating that vulnerability is "everywhere" online, P7 implies that this vulnerability is unavoidable and inherent to social media, especially given the impossibility of true and complete privacy in online environments that require some degree of information sharing [82]. P7 thus suggests that, lacking privacy, one is always vulnerable in that they are open to both feedback and content circulation on social media, for better or worse. Similarly, P14 (man, bisexual, Black) explained:

> I think probably anyone who willingly goes on social media and shares part of their lives, regardless of what it is, is making the decision to be visible, even if it's not a conscious decision. I think that is something that definitely needs to be thought about more. I think a lot of times now, because the world is so used to technology, if you don't really think about how much of ourselves we're sharing online and what that could mean for us in the future. The future possible repercussions of that is it can be dangerous.

P14 thus implied a sort of acquiescence to the inherent vulnerability of being visible on social media, as well as a perception that this vulnerability was not already dangerous but could become so, and thus could shift toward undesired vulnerability and harm. P5 (man, queer, Asian/Hong Kong) expanded on this acquiescence or assumed vulnerability, saying:

> Being visible, and being vulnerable, in my opinion, is to kind of accept that different opinions exist and that they're going to exist within your realm of existence, and it's a different tactic to just accept those criticisms and perspectives.

In this example, vulnerability is akin to being "open" to encountering differing perspectives. We note, however, that vulnerability to a difference of opinion is not representative of all possible vulnerabilities and related outcomes on social media.

In another sense, individuals may experience ambivalent vulnerability by balancing desired and undesired aspects of vulnerability. For example, P19 (woman, Hispanic/Puerto Rican), a blogger, noted:

> Definitely, when I started my blog, it's like, a bunch of different things where I want to say that I'm a poet, I'm a foster kid, I am a first-generation college student. And these are things that like, are true, and I'm very proud of, but at the same time, will open the door for a lot of people to come in and give me judgment. And it makes me feel vulnerable. It's like opening my, like, opening myself to these conversations. But at the same time, I feel like I'm taking away from the world, if I don't allow people to see that this is something you can do. Like, you can be a foster kid, and you can go get education, and you can have a really high GPA, you could do all these things. And

> that's like, the issue is like, you really want to be authentic. But at the same time, when you do it, you are putting yourself at risk. So, I do feel very vulnerable at times.

In this example, P19 reflects on revealing (potentially) stigmatized identities and weighing the risks of judgment and contributing to stigma through silence against the potential benefits of authentic self-expression, destigmatization, and supporting others [38]. Ultimately, P19 balanced the desire for identity expression and the ability to motivate others with awareness of risks to create a more ambivalent conceptualization of online vulnerability.

We argue that the unavoidable, unspecified vulnerability of being on social media referenced in these quotes is akin to vulnerability as ambivalent and is significantly different from vulnerabilities associated with specific sources, as well as from explicitly un/desired vulnerability described earlier. In being unavoidable, the *ambivalent* vulnerability category captures aspects of inherent vulnerability as defined by Mackenzie et al. [70] but does not speak to corporeal vulnerability in its totality. By explicitly considering multiple valences of vulnerability, including alternatives to undesired and desired, we can better discern how vulnerability varies across spaces and information types (*i.e.*, what is visible), how vulnerability valences inform identity visibility motivations, and how interactions between social and technical dimensions of social media shape perceived vulnerability.

4.3.3 Desired Vulnerability. In addition to instances of undesired and ambivalent vulnerability, participants acknowledged vulnerability that they considered desirable, were willing to assume, and/or perceived as potentially benefitting themselves or others.

Participants sometimes understood vulnerability broadly as desirable; this framing in turn informed what information or identities they shared and with what intent. P2 (woman, bisexual, White), for instance, clarified her perspective on vulnerability broadly:

> I think being vulnerable can be a good word, I think. And a lot of people think it's a bad thing, but I think it's actually really positive in most situations, if you're consenting to be vulnerable, and if there's a purpose for you, and things like that, I would say I am more vulnerable when I actually share.

As identified by P2, consent and control were important factors in determining whether vulnerabilities were desired or undesired. Sociotechnical environments influenced participants' perceptions of consent and control, which in turn influenced the valence they attributed to their own vulnerability. For instance, some participants turned to secondary accounts with more insular audiences to engage in desired vulnerability. P11 (non-binary, queer, Black) describes this, saying:

> Because on my public [Instagram] I'm a very happy go lucky, cheery person. But on my private Instagram, I feel like they actually know more about me. And that's like, what shines through because on there, I'll tell them everything. I'll be like, 'My mom is getting on my nerves, school's getting on my nerves. I was in the hospital last week. Like I'm just having a really hard time.'

By managing their content's privacy and visibility, P11 created a space for authentic expression and venting; this example suggests one way that desired vulnerability may yield beneficial outcomes, such as catharsis or emotional validation [6, 18, 31, 52]. Whether vulnerability was understood as desired was also intimately shaped by one's identities and experiences. P13 (woman, bisexual, Black), who lived with cancer, explained:

> Yeah, I mean, for me, you know, being visible on social media really is a good thing. And, you know, of course, I couldn't have found that before the cancer diagnosis, you know, and if it's kind of too bad that it took getting cancer in order to get to that place, but you know, [...] I have to figure that there are a lot of people who never get there, you know, where they can totally be themselves.

In P13's experience, the vulnerability associated with breast cancer reframed her understanding of and desire to be vulnerable on social media. This experience resulted in P13's practice of intentional identity visibility on Facebook, which was associated with benefits such as social support. Later, P13 related the experience of posting about the discomfort associated with feeling that her independence was compromised due to rising anti-Black violence, explaining, *"That's something that I feel was taken away from me, you know, and so I shared about that, and just received lots of, lots of support."* Desired or consented-to vulnerability may thus be strategically enacted via social media platforms to achieve outcomes ranging from social support exchange to clarification of identities and experiences.

While enacted desired vulnerability enabled participants to reap social support benefits, they were also able to support others via their representation of marginalized or stigmatized identities and experiences. For example, P5 (man, queer, Asian/Hong Kong) used his Twitter account to *"harness that power, if you will, to make sure that not just, not just to represent myself, but also to represent people who might share my different identities,"* while P10 (woman, straight, Hispanic) created YouTube videos about their skin condition because *"it could be helpful to somebody else who's maybe going through the same thing."* Research shows that this form of vulnerable identity visibility can facilitate social connection and support for those with stigmatized identities and experiences [15]. Beyond identity specifically, leveraging vulnerability to facilitate a sense of connection, as described by P18 (woman, Latina/Mexican American), is critical in times of social isolation, such as that exacerbated by the global COVID- 19 pandemic:

> And I think because I've like been a little more vulnerable with what I've shared on social media, it makes it so that, like, there are folks that will like pop in with just like a, you know, 'You've got this,' like, 'You're doing a great job' or with like, the latest thing has been like, 'Hey, like, we're actually having a zoom meeting, like later this week, if you want to jump on, and we're just gonna like chit chat and catch up or whatever.' And it's like, 'Yeah, let's do it.' Like, I want to be a part of that, like, social interaction, even though we're kind of limited right now.

In sum, conceiving vulnerability as sometimes desired helps us understand how individuals do not only passively experience vulnerability but also deliberately and strategically enact it to achieve personal, social, and societal goals. In attending to the particularities of social media contexts and vulnerability as facilitating beneficial and harmful outcomes, the FSMV taxonomy extends Mackenzie et al.'s [70] feminist taxonomy to social media. It also contributes a more nuanced analysis of vulnerability sources, states, and valences, which are visualized in Figure 2 below. Finally, our emphasis on identity visibility and self-revelation intimates how social positionality further informs perceived vulnerability and how a feminist-informed taxonomy, such as the FSMV taxonomy, may advance understanding of how social power interacts with and through social media.

5 DISCUSSION

This paper contributes the Feminist Social Media Vulnerability (FSMV) taxonomy. Through this novel taxonomy, we make the following contributions:

- Conceptualize social media vulnerability in a way that (1) is grounded in feminist philosophy, thereby expanding Mackenzie et al.'s feminist taxonomy [70] to the social media context and accounting for observation as well as direct experience as informing vulnerability; (2) draws on dialectical perspectives on disclosure, privacy, and self-presentation relevant to social computing to consider conceptualizations of vulnerability beyond risk and harm; and

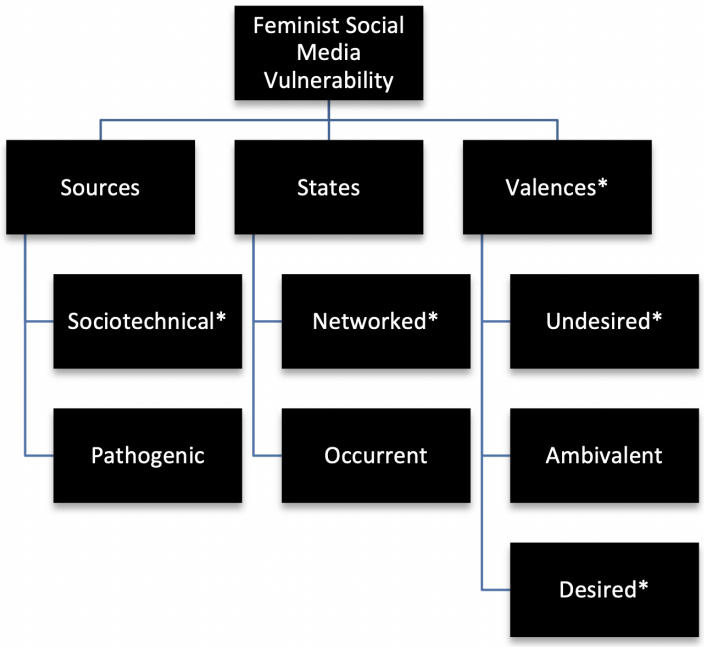

Fig. 2. A conceptual feminist taxonomy of social media vulnerability. Terms followed by an asterisk (*) denote conceptual categories we introduce in this work. Other conceptual categories are derived from Mackenzie et al.'s [70] feminist taxonomy of vulnerability and Gilson's [47] work on vulnerability.

(3) accounts for sociotechnical spaces as both context and actor, thereby providing a unifying framework for examining vulnerability on social media
- Reorient social media vulnerability as a condition of "openness to being affected by and affecting others" [47] that facilitates a range of outcomes
- Challenge paternalistic determinations of vulnerability by explicitly situating perception within vulnerability
- Introduce *networked vulnerability* as a state of vulnerability in sociotechnical contexts
- Introduce *valence*, including *undesired*, *ambivalent*, and *desired*, as a dimension of vulnerability

We expand on these contributions in the following sections.

5.1 Theoretical Contributions

Through the FSMV taxonomy, we define social media vulnerability as a condition of openness that is (1) perceived through networked interactions, (2) perpetrated or enabled by individual and sociotechnical actors (i.e., users and platforms), (3) informed by factors including identity, social positionality, and stigma, and (4) may be perceived as un/desired or met with ambivalence by an individual. The FSMV taxonomy contributes *sociotechnical* as a source, *networked* as a state, and *ambivalent* and *(un)desired* as valences of vulnerability encountered (i.e., observed and experienced) on social media. These additional categories draw on feminist framings of vulnerability as openness [47, 86], aid in extending feminist taxonomic perspectives [70] to sociotechnical contexts, and move

toward a unified framework for examining disclosure, privacy, identity visibility, and harm on social media.

By specifying *sociotechnical* as a source of vulnerability, in addition to pathogenic, we can situate digital contexts as both enabling and perpetrating vulnerability [100]. While we borrow the verbiage of platform-enabled and platform-perpetrated from Schoenebeck & Blackwell [100], it is important to note that we transpose these terms to the context of vulnerability broadly instead of harm specifically. Distinguishing between platforms as context and actors allows more nuanced theorizing of vulnerability. Identifying platforms as actors that bear on vulnerability may contribute to holding platforms accountable for vulnerability as harm and surface additional ways that platform architecture upholds hierarchies of social power and oppression.

While prior work speaks to effects of the networked nature of social media (*e.g.*, [6, 15, 20, 23, 45, 57, 72, 110]), our concept of *networked vulnerability* extends these perspectives to more explicitly consider the role of individuals' perception in vulnerability as well as to address the temporality of vulnerability on social media. We argue that networked vulnerability expands vulnerability beyond direct experience to consider the *observed* vulnerability of others as deeply influential to the perceived vulnerability of the self; the perceived vulnerability of self in turn influences self-presentation and identity visibility practices. We thus define *networked vulnerability* as a state in which one's perceived vulnerability is informed by and/or contributes to another's. Furthermore, as observation and perceived vulnerability inform behavior, we contend that networked vulnerability blurs the boundaries between temporally-defined states of vulnerability, such as dispositional (*i.e.*, potential) and occurrent (*i.e.*, experienced) vulnerability, as outlined by Mackenzie et al. [70]. While vulnerability via observation can occur offline as well, we posit that the networked and masspersonal [81] nature of social media differs from offline contexts such that *networked vulnerability* on social media warrants further attention.

Finally, in positioning valence as an attribute of social media vulnerability, we challenge associations between vulnerability and harm/violence evident in prior theorization. In keeping with a feminist critique of vulnerability, we argue for conceiving of vulnerability as a condition of "openness" [47, 86] and facilitating a range of outcomes that include and extend beyond harm. While the two concepts are often used interchangeably, and harm remains a central concern of HCI scholarship, parsing out the two is fundamental to developing a more robust understanding of vulnerability (and harm) as it plays out on social media. Harm is perceived broadly in HCI as an undesirable outcome that varies in severity based on factors ranging from intent to scale [98] and, more specifically, as a negative outcome that *cannot be resisted* [114]. Vulnerability, however, can be more appropriately framed as openness to affecting/being affected that can result in (un)desired outcomes (including harm) and can be strategically leveraged and/or managed (albeit to different extents in part resulting from one's social positionality). As previously noted, addressing the severity of vulnerability is beyond this project's scope. The addition of valence to vulnerability also nods to the tension between risk and benefit that appears central in dialectical perspectives on disclosure and privacy (*e.g.*, [38, 87]) and further discourages alignment of vulnerability with solely harm. This move has additional implications for social power and positionality in vulnerability research, which we expand on in *section 5.3*.

Following Nickerson et al. [79], we assert that the proposed FMSV taxonomy reflects several attributes of a useful taxonomy. The FMSV is *concise* in proposing only three dimensions of vulnerability (*e.g.*, source, state, and valence); *robust* in that the included dimensions and characteristics clearly differentiate experiences/types of vulnerability, holds space for understandings of vulnerability as desired, and considers social media platforms as actors and contexts with respect to vulnerability; and *explanatory* in that the dimensions and characteristics may be used to better

understand experiences of vulnerability on social media. Put another way, experiences of vulnerability may be located in the taxonomy [13, 79]. We acknowledge that whether the FMSV taxonomy is *comprehensive* (*i.e.*, "can classify all known objects within the domain under consideration"; [79]) and *extendible* (*i.e.*, "allow[s] for inclusion of additional dimensions and new characteristics"; [79]) cannot be determined through this study alone. In building on Mackenzie et al.'s [70] feminist taxonomy of vulnerability and drawing on interdisciplinary understandings of vulnerability and harm, however, the FMSV provides a foundation through which experiences of vulnerability may be analyzed and upon which additional dimensions, characteristics, and understandings of social media vulnerability may be built.

5.2 Revisiting Applications of Vulnerability in HCI

Social computing work increasingly deploys the concept of vulnerability [10, 46, 73, 77, 106, 112]. More specifically, scholars invoke the concept of vulnerability to describe "vulnerable populations," both in terms of the challenges they face in sociotechnical contexts and in the challenges researchers face in engaging with them. For instance, scholars suggest that working with vulnerable populations necessitates attention to ethics and privacy in research design in a way that less vulnerable populations do not, and posit ethical questions researchers should ask of ourselves as we work with these populations [10]. However, insights from the FSMV taxonomy could help researchers more productively frame these populations and their challenges. First, the "vulnerable population" framing assumes that certain groups are inherently vulnerable (implying that others are not). This deterministic assumption becomes problematic when coupled with framings of vulnerability as synonymous with harm [74, 98, 100]. The FSMV taxonomy challenges the designation of social groups as inherently and perpetually vulnerable to harm by acknowledging both that (1) all humans experience innate or inherent vulnerability as an aspect of human nature *and* (2) certain situational factors (including sociotechnical ones) can inhibit or exacerbate inherent vulnerabilities. These acknowledgments aid in maintaining focus on the social and situational factors that influence vulnerability, avoid paternalistic interpretations of vulnerability, and—in reframing vulnerability to refer to an ambivalent condition of openness—creates space for individual agency and resistance within vulnerability. Moreover, this framing of vulnerability implores *all* researchers—not just those working with populations deemed vulnerable by external entities like Institutional Review Boards—to explicitly grapple with questions of ethics and privacy in their research endeavors above and beyond fulfillment of longstanding benchmarks like the Belmont Principles [113].

Further, in emphasizing perception in vulnerability, the FSMV taxonomy highlights individual experience as a factor that shapes perceptions and experiences of vulnerability. In attending to individual sensemaking and perception of vulnerability, the FSMV taxonomy acknowledges how social position and identity (and stigma and stereotypes, by extension) bear on individual perception. We argue that acknowledging both individual perception and social context as influences on social media vulnerability contributes to greater nuance and depth in analyses and advances the potential for a critical understanding of vulnerability. Thus, rather than framing a population at large as vulnerable, alternative framings, such as that offered by the FSMV taxonomy, can better account for the individual, situational, and often systemic factors that play prominent roles in shaping experiences of vulnerability on social media.

We suggest that CSCW researchers working with "vulnerable populations" consider specifying on what dimensions these populations experience vulnerability. Doing so would aid in (1) avoiding paternalistic and deterministic labeling of entire populations as vulnerable, and (2) understanding what specifically factors into individuals' and populations' experiences with vulnerability. Additionally, attending to how individuals valence vulnerability, as is facilitated by the FMSV, deepens our understanding of behavior on, and in interactions with, social media. Insights into salient

dimensions, sociotechnical contexts (*e.g.*, affordances, algorithmic systems, platform perceptions), and valences of vulnerability may be leveraged in design to mitigate undesired vulnerability without constraining users' abilities to strategically leverage vulnerability in desired ways.

We also advocate that CSCW researchers could leverage the specific dimensions of networked vulnerability in future work. Rather than considering vulnerability as a phenomenon that solely emanates from direct and harmful interpersonal interactions, researchers should be open to the ways in which the networked nature of social media can facilitate more vicarious experiences of vulnerability. Finally, this taxonomy can help us understand vulnerability not just as a phenomenon that exists in interpersonal interactions (as is typically considered in disclosure literature) or interactions with platforms (which is typically considered in privacy and security literature) but as a multidimensional phenomenon encompassing interactions with *and* on social media.

5.3 Power and Social Position within Vulnerability

We ground our proposed taxonomy in feminist theory to further embed considerations of power and oppression within vulnerability. Although we adopt the view that vulnerability is more productively framed as ambivalent than as synonymous with risk and harm, we maintain that identity and social power deeply inform experiences (including harm) and perceptions of social media vulnerability. Our analysis identifies some of these connections between vulnerability and power.

Within the sociotechnical source category, particularly concerning platform-enabled vulnerabilities, we (and others [91, 100]) note that the features and affordances of social media that enable finding and connecting with others may be leveraged to maintain the same power dynamics that exist in offline interactions. Regardless of identity and background, participants shared the perception that vulnerability was endemic to all social media. That said, the perception and, in some cases, the reputation of certain platform userbases as prejudiced toward particular identities (*e.g.*, Reddit users as misogynistic) influenced which identities participants chose to make visible and where. Further, participants' comments regarding shadowbanning illustrate algorithmic symbolic annihilation [7, 61] and intimate how platforms as actors further shape user behavior. Engaging social media users' perceptions of vulnerability can aid in illuminating the intersecting social, technical, and procedural/governance factors and subtle power dynamics that inform platform adoption and disuse as well as online community development and dissolvement. Scholarship has acknowledged that identity, particularly socioeconomic identity, can influence platform adoption and abandonment/non-use (*e.g.*, [16, 53, 54]). The FSMV taxonomy contributes to this body of work by providing a framework through which sources of and influences on vulnerability can be identified and analyzed through a social positionality lens. Perhaps more importantly, beyond binary understandings of adoption and abandonment, attention to experiences of vulnerability as we propose offers insights into gradations in use patterns and behaviors that inform and are informed by perceived and experienced vulnerability.

As shown in connection to networked vulnerability, individuals do not need to directly experience vulnerability on social media to be affected by it. Observing others being vulnerable and outcomes thereof can inform perceptions of one's own vulnerability and/or constitute harm (as works such as [23] also argue). Participants reported self-silencing, feeling as if they did not belong, and feeling unsafe without directly experiencing consequences to vulnerability. While our intent is not to advocate for complete self-visibility on social media, the fact that participants felt unsafe sharing their gender, sexuality, and political identities within their networks speaks to the myriad connections between visibility, vulnerability, identity, and power on social media. Accounting for observed/networked vulnerability in research areas such as online harm, harassment, destigmatization, and self-presentation can further illuminate the social ramifications of individual behavior online.

While research points to experiences of harassment (or occurrent pathogenic vulnerability, according to the FSMV taxonomy) as influential to subsequent platform use and withdrawal [28], we argue that focusing only on occurrent vulnerability and neglecting networked vulnerability paints an incomplete picture of how vulnerability and/or harmful interactions shape individuals' self-presentation decisions on social media. Networked vulnerability posits that online harm is *sometimes* enacted but *often* a vicarious experience, which (1) can expand scholars' conceptual understanding of the scope and impact of online harassment and undesired vulnerability, and (2) can encourage scholars to think about the kinds of remediating practices that can effectively redress not only occurrent, but also undesired networked vulnerability online. While Schoenebeck et al. [101] draw from justice theories to highlight the remediation preferences of those who directly experienced harassment, expanding our view and considering the preferences of those who experience vicarious harm through the networked nature of social media can potentially unearth a more comprehensive array of social and technological mechanisms for redressing harm on a large scale.

In framing vulnerability as openness to affecting/being affected, the FSMV taxonomy may similarly be used in projects that consider how mechanisms of networked vulnerability may be leveraged to foster beneficial and social outcomes, such as destigmatization. Our inclusion of valence as a dimension of social media vulnerability highlights the potential for social media to not only reinforce social hierarchies and interpersonal violence, but also to *challenge* these outcomes through leveraging visibility and vulnerability to validate others, forge connection, and facilitate social support.

In combination, our findings and resulting taxonomy suggest ways that power and vulnerability interact at individual levels, how individuals may leverage vulnerability to challenge power and enact resistance, and how power and vulnerability interact and act on social levels.

5.4 Implications for Design and Platforms

Our analysis and development of the FMSV taxonomy have several implications for social media design, including the need for more granular controls over content and profile visibility, default privacy settings, and content consumption; within discussion of granularity, we point to the importance of temporality in control. We also reflect on implications of the FSMV for platforms and platform governance.

5.4.1 Granular controls over content and profile visibility over time. Findings regarding sociotechnical sources of vulnerability underscore a need for more granular user controls over *content* and *profile* visibility and the degree to which networked and non-networked others can interact with one's content and profile. Participants in this study expressed concern regarding non-networked others being able to find and respond to content in unexpected ways, as well as regarding exposing others to their own desired vulnerability without others' consent. Finer control over (1) privacy settings, such as the ability to easily toggle between public and private accounts and individual posts and (2) audience, including who may reply to or share content, may assuage users' concerns about undesired sociotechnical and networked vulnerability. The need for more granular visibility and interaction settings is echoed in research conducted with marginalized social media users [32, 50].

We additionally suggest that allowing settings to persist over time by default—such as allowing content posted when a user had their account set to private to remain private *by default* if one switches to a public profile—would provide greater control over un/desired vulnerability. Recent work suggests that users engage in laborious strategies such as deleting past content and soft blocking when switching from private to public accounts on Twitter [62]. Our participants also

reported deleting past content when the audience it reaches is misaligned with the poster's imagined audience (*e.g.*, P5 who tweeted about popular YouTuber PewDiePie). Moreover, our participants described the adoption of both public and private accounts on social media as facilitating desired vulnerability (*e.g.*, P2 who created a private Instagram account for kink-related content). Honoring the privacy setting under which *a particular piece of content* was posted, even when one switches *account* settings, may (1) offset some of the labor involved in attempts to minimize one's potential for experiencing undesired vulnerability on social media, and (2) enable users to more easily create the kinds of social media environments that facilitate enactment of desired vulnerability.

5.4.2 Granular control over content consumption. Our explication of networked vulnerability indicates the potential for finer user control over content users *consume*, above and beyond control over what content users *produce*. Participants suggested that consumption of content that espoused negativity, hate, and harassment to others holding a similar identity as them influenced their experience of vulnerability on social media (*e.g.*, P17 who described the "pussy pass" subreddit). Greater control over what kinds of content a user consumes and when they consume it may help to curb undesired vulnerability. Features such as disabling video auto-play by default, bolstering content warning systems, and increasing similar proactive indicators of sensitive content may aid in reducing undesired networked vulnerability. Previous research on visibility control supports these notions, as perceived control appears to influence where social media users choose to be visible [18, 116] and how [4, 8, 21, 67, 109]. Additionally, designers could make it easier for individuals to curate a more human-centered news feed [6] by selecting topics that they are/are not interested in seeing at particular times in the day/week. Given the alignment between dialectic perspectives on online disclosure and vulnerability as openness, as we suggest in this paper, we argue that greater control over visibility extends to allowing social media users to create spaces, including through content curation, for desired vulnerability.

5.4.3 Holding platforms responsible. Emphasis on user controls and consent, however, does not diminish the responsibility of platforms/social media companies for harm the platform itself perpetrates against users. Indeed, in positioning platforms and algorithmic systems as actors as well as contexts, the FMSV taxonomy highlights platforms as a *source* of vulnerability. Holding space for platforms as actors is significant in that the FMSV may be used to identify how platforms—through design changes, defaults, and policies—affect (*i.e.*, contribute to or ameliorate) user vulnerability (and with what valence). While holding platforms accountable for vulnerability is not the focus of this paper, we note, however, that being able to identify actors (including platforms) as responsible for undesired vulnerability is a necessary step in holding such actors accountable and redressing harm. In drawing on feminist philosophical framings of vulnerability that are grounded in understandings of vulnerability as resistance against oppression, as well as understandings of online harm that similarly identify platforms as potential perpetrators (*i.e.*, [100]), we argue that the FMSV may be used in conjunction with and to further trauma-informed approaches to computing, including affirmative consent frameworks [56] and alternative justice models of platform governance [100]. In other words, the FMSV may be used—by platforms and social media users—to locate platforms as actors and contextual influences on vulnerability (in accordance with [13, 79]) and in a way that is compatible with these burgeoning approaches to platform governance and accountability.

5.5 Reflections and Future Possibilities

While we purposefully recruited a sample that embodied diverse and sometimes multiply marginalized social identities, we did not employ an intersectional analysis [99], which could elucidate further mechanisms of or additional taxonomic categories of vulnerability. Future research may

assess and refine the FSMV taxonomy in connection with specific intersections of identities and/or experiences.

Additionally, we intentionally recruited U.S.-based social media users to provide a more consistent context of identity-informed social positionality, power, and marginality. Future research should explore how our findings may extend to or be challenged in social and cultural contexts beyond what we studied. Recent work suggests that perceptions of the severity of harmful content online differ based on national context [59]; understanding how these national contexts influence perceptions of vulnerability online more broadly constitute a worthwhile avenue for future research and might allow further expansion of the FSMV taxonomy.

Moreover, there are ample opportunities to explore social media vulnerability using an amalgamation of research methods, including but not limited to surveys to assess the generalizability of our findings and validate our proposed taxonomy, and ethnographic work to understand vulnerability in practice in social media spaces.

We also acknowledge that, although grounded in feminist philosophy, we do not engage in- depth with vulnerability's ethical and moral dimensions. In situating vulnerability in a critical, feminist framework, Mackenzie et al. [70], for instance, pose the question, "Who bears responsibility for vulnerability?" In social media contexts, as elucidated by our findings, we posit that responsibility could fall to various parties, including individual users, platforms themselves, and policymakers. We encourage researchers to engage with this question in future vulnerability theory-building.

6 CONCLUSION

We contribute the Feminist Social Media Vulnerability (FSMV) taxonomy, which extends and complicates prior work on vulnerability rooted in face-to-face interactions. While prior taxonomies of vulnerability invoke categories like sources and states that extend to social media environments, the sociotechnical dynamics of these environments necessitate new subcategories, such as *sociotechnical* situational sources of vulnerability and the state of *networked* vulnerability—categories we identify through our analysis. Our findings additionally reveal the salience of *valence* in perceived vulnerability and demonstrate how conceptualizations of vulnerability can move beyond risk and harm to contend with the ways that social media vulnerability presents as openness and may be regarded as *ambivalent*, *desirable*, and *undesirable*.

We define social media vulnerability as a condition of openness that is (1) perceived through networked interactions, (2) perpetrated or enabled by individual and sociotechnical actors (i.e., users and platforms including algorithms and affordances), (3) informed by factors including identity, social positionality, and stigma, and (4) may be perceived as un/desired or met with ambivalence by an individual. Overall, this taxonomy builds on and extends feminist philosophy, communication, and social computing literature to parse out the disparate experiences of vulnerability faced by different individuals and social groups with varying proximity to power and root vulnerability within individuals' lived experiences and sensemaking thereof. We propose the FSMV as a unifying taxonomy that can inform future more systematic and nuanced investigations of vulnerability and social media both in scholarship (and thus facilitating comparisons and synthesis across studies) and design explorations. Future research may use this taxonomy to interrogate the ethics of social media vulnerability, asking and answering questions around who bears responsibility for vulnerability and for mitigating undesired vulnerability. Finally, designers may leverage these findings to develop social media features that give users finer control over content and profile visibility, default privacy settings, and content consumption.

ACKNOWLEDGMENTS

We are deeply grateful to participants for trusting in us and sharing their experiences. We also thank the anonymous ACM ACs and reviewers for their thoughtful feedback. Finally, we thank Dr. Carol F. Scott, Dr. Kentaro Toyama, and Yulin Yu for feedback on earlier drafts of this work.

REFERENCES

[1] Joseph A. Allen, Tammy Beck, Cliff W. Scott, and Steven G. Rogelberg. 2014. Understanding workplace meetings: A qualitative taxonomy of meeting purposes. *Management Research Review* 37, 9 (Aug. 2014), 791–814. https://doi.org/10.1108/MRR-03-2013-0067

[2] Irwin Altman and Dalmas A. Taylor. 1973. *Social penetration: The development of interpersonal relationships.* Holt, Rinehart & Winston, Oxford, England. Pages: viii, 212.

[3] Nazanin Andalibi. 2019. What Happens After Disclosing Stigmatized Experiences on Identified Social Media: Individual, Dyadic, and Social/Network Outcomes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3290605.3300367

[4] Nazanin Andalibi. 2020. Disclosure, Privacy, and Stigma on Social Media: Examining Non-Disclosure of Distressing Experiences. *ACM Transactions on Computer-Human Interaction* 27, 3 (June 2020), 1–43. https://doi.org/10.1145/3386600

[5] Nazanin Andalibi. 2021. Symbolic annihilation through design: Pregnancy loss in pregnancy-related mobile apps. *New Media & Society* 23, 3 (March 2021), 613–631. https://doi.org/10.1177/1461444820984473 Publisher: SAGE Publications.

[6] Nazanin Andalibi and Andrea Forte. 2018. Announcing Pregnancy Loss on Facebook: A Decision-Making Framework for Stigmatized Disclosures on Identified Social Network Sites. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, Montreal QC Canada, 1–14. https://doi.org/10.1145/3173574.3173732

[7] Nazanin Andalibi and Patricia Garcia. 2021. Sensemaking and Coping After Pregnancy Loss: The Seeking and Disruption of Emotional Validation Online. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (April 2021), 1–32. https://doi.org/10.1145/3449201

[8] Nazanin Andalibi, Margaret E. Morris, and Andrea Forte. 2018. Testing Waters, Sending Clues: Indirect Disclosures of Socially Stigmatized Experiences on Social Media. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (Nov. 2018), 19:1–19:23. https://doi.org/10.1145/3274288

[9] Nazanin Andalibi, Pinar Ozturk, and Andrea Forte. 2017. Sensitive Self-disclosures, Responses, and Social Support on Instagram: The Case of #Depression. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17)*. Association for Computing Machinery, New York, NY, USA, 1485–1500. https://doi.org/10.1145/2998181.2998243

[10] Alissa N. Antle. 2017. The ethics of doing research with vulnerable populations. *Interactions* 24, 6 (Oct. 2017), 74–77. https://doi.org/10.1145/3137107

[11] Carolina Are. 2020. How Instagram's algorithm is censoring women and vulnerable users but helping online abusers. *Feminist Media Studies* 20, 5 (July 2020), 741–744. https://doi.org/10.1080/14680777.2020.1783805 Publisher: Routledge _eprint: https://doi.org/10.1080/14680777.2020.1783805.

[12] Carolina Are. 2021. The Shadowban Cycle: an autoethnography of pole dancing, nudity and censorship on Instagram. *Feminist Media Studies* (May 2021), 1–18. https://doi.org/10.1080/14680777.2021.1928259

[13] Kenneth D. Bailey. 1994. *Typologies and taxonomies: an introduction to classification techniques.* Number 07-102 in Quantitative applications in the social sciences. Sage Publications, Thousand Oaks, Calif.

[14] Michele Banko, Brendon MacKeen, and Laurie Ray. 2020. A Unified Taxonomy of Harmful Content. In *Proceedings of the Fourth Workshop on Online Abuse and Harms*. Association for Computational Linguistics, Online, 125–137. https://doi.org/10.18653/v1/2020.alw-1.16

[15] Kristen Barta. 2021. Beacons over bridges: hashtags, visibility, and sexual assault disclosure on social media. *Information, Communication & Society* 0, 0 (Aug. 2021), 1–18. https://doi.org/10.1080/1369118X.2021.1962946 Publisher: Routledge _eprint: https://doi.org/10.1080/1369118X.2021.1962946.

[16] Eric P. S. Baumer. 2018. Socioeconomic Inequalities in the Non use of Facebook. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, Montreal QC Canada, 1–14. https://doi.org/10.1145/3173574.3174190

[17] Leslie A. Baxter and Barbara M. Montgomery. 1996. *Relating: Dialogues and Dialectics.* Guilford Press. Google-Books-ID: RG6EujhALsEC.

[18] Natalya N. Bazarova and Yoon Hyung Choi. 2014. Self-Disclosure in Social Media: Extending the Functional Approach to Disclosure Motivations and Characteristics on Social Network Sites. *Journal of Communication* 64, 4 (Aug. 2014), 635–657. https://doi.org/10.1111/jcom.12106

[19] Jeremy Birnholtz, Ashley Kraus, Weiwei Zheng, David A. Moskowitz, Kathryn Macapagal, and Darren Gergle. 2020. Sensitive Sharing on Social Media: Exploring Willingness to Disclose PrEP Usage Among Adolescent Males Who Have Sex With Males. *Social Media + Society* 6, 3 (July 2020), 205630512095517. https://doi.org/10.1177/2056305120955176

[20] DANAH BOYD. 2010. Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications. In *A Networked Self*. Routledge. Num Pages: 20.

[21] danah boyd. 2014. *It's Complicated: The Social Lives of Networked Teens*. Yale University Press, New Haven London.

[22] Elizabeth H. Bradley, Leslie A. Curry, and Kelly J. Devers. 2007. Qualitative Data Analysis for Health Services Research: Developing Taxonomy, Themes, and Theory. *Health Services Research* 42, 4 (Aug. 2007), 1758–1772. https://doi.org/10.1111/j.1475-6773.2006.00684.x

[23] André Brock Jr. 2020. *Distributed Blackness*. New York University Press. http://www.degruyter.com/document/doi/10.18574/9781479811908/html Publication Title: Distributed Blackness.

[24] Sarah L. Buglass, Jens F. Binder, Lucy R. Betts, and Jean D.M. Underwood. 2016. When 'friends' collide: Social heterogeneity and user vulnerability on social network sites. *Computers in Human Behavior* 54 (Jan. 2016), 62–72. https://doi.org/10.1016/j.chb.2015.07.039

[25] Judith Butler. 2016. Rethinking Vulnerability and Resistance. In *Vulnerability in Resistance*, Judith Butler, Zeynep Gambetti, and Leticia Sabsay (Eds.). Duke University Press, 12–27. http://www.degruyter.com/document/doi/10.1515/9780822373490-004/html Pages: 12-27 Publication Title: Vulnerability in Resistance Section: Vulnerability in Resistance.

[26] John L. Campbell, Charles Quincy, Jordan Osserman, and Ove K. Pedersen. 2013. Coding In-depth Semistructured Interviews: Problems of Unitization and Intercoder Reliability and Agreement. *Sociological Methods & Research* 42, 3 (Aug. 2013), 294–320. https://doi.org/10.1177/0049124113500475

[27] Caleb T. Carr and Rebecca A. Hayes. 2015. Social Media: Defining, Developing, and Divining. *Atlantic Journal of Communication* 23, 1 (Jan. 2015), 46–65. https://doi.org/10.1080/15456870.2015.972282 Publisher: Routledge _eprint: https://doi.org/10.1080/15456870.2015.972282.

[28] Kalyani Chadha, Linda Steiner, Jessica Vitak, and Zahra Ashktorab. 2020. Women's Responses to Online Harassment. *International Journal of Communication* 14, 1 (2020), 239–257. https://ijoc.org/index.php/ijoc/article/view/11683/2906

[29] Stevie Chancellor, Nazanin Andalibi, Lindsay Blackwell, David Nemer, and Wendy Moncur. 2019. Sensitive Research, Practice and Design in HCI. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems (CHI EA '19)*. Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/3290607.3299003

[30] Stephenie R. Chaudoir and Jeffrey D. Fisher. 2010. The disclosure processes model: Understanding disclosure decision making and postdisclosure outcomes among people living with a concealable stigmatized identity. *Psychological Bulletin* 136, 2 (2010), 236–256. https://doi.org/10.1037/a0018193 Place: US Publisher: American Psychological Association.

[31] Stephenie R. Chaudoir and Diane M. Quinn. 2010. Revealing concealable stigmatized identities: The impact of disclosure motivations and positive first disclosure experiences on fear of disclosure and well-being. *The Journal of social issues* 66, 3 (Sept. 2010), 570–584. https://doi.org/10.1111/j.1540-4560.2010.01663.x

[32] Janet X. Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin A Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. 2022. Trauma-Informed Computing: Towards Safer Technology Experiences for All. In *CHI Conference on Human Factors in Computing Systems*. ACM, New Orleans LA USA, 1–20. https://doi.org/10.1145/3491102.3517475

[33] Nancy L. Collins and Lynn Carol Miller. 1994. Self-disclosure and liking: A meta-analytic review. *Psychological Bulletin* 116, 3 (1994), 457–475. https://doi.org/10.1037/0033-2909.116.3.457 Place: US Publisher: American Psychological Association.

[34] William D. Crano, Marilynn B. Brewer, and Andrew Lac. 2014. *Principles and methods of social research* (third edition ed.). Routledge, New York.

[35] Valerian J. Derlega and Janusz Grzelak. 1979. Appropriateness of self-disclosure. In *Self-disclosure: Origins, patterns, and implications of openness in interpersonal relationships*, Gordon J. Chelune (Ed.). Jossey-Bass, San Francisco, 151–176.

[36] Michael A. DeVito, Jeremy Birnholtz, Jeffery T. Hancock, Megan French, and Sunny Liu. 2018. How People Form Folk Theories of Social Media Feeds and What it Means for How We Study Self-Presentation. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, Montreal QC Canada, 1–12. https://doi.org/10.1145/3173574.3173694

[37] Michael A. Devito, Ashley Marie Walker, Jeremy Birnholtz, Kathryn Ringland, Kathryn Macapagal, Ashley Kraus, Sean Munson, Calvin Liang, and Herman Saksono. 2019. Social Technologies for Digital Wellbeing Among Marginalized Communities. In *Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing (CSCW '19)*. Association for Computing Machinery, New York, NY, USA, 449–454. https://doi.org/10.1145/3311957.3359442

[38] Kathryn Dindia. 1998. 'Going into and coming out of the closet': The dialectics of stigma disclosure. In *Dialectical Approaches to Studying Personal Relationships*, Barbara M. Montgomery and Leslie A. Baxter (Eds.). Lawrence Erlbaum Associates, Mahwah, NJ, 83–107.

[39] Brooke Erin Duffy and Ngai Keung Chan. 2019. "You never really know who's looking": Imagined surveillance across social media platforms. *New Media & Society* 21, 1 (Jan. 2019), 119–138. https://doi.org/10.1177/1461444818791318 Publisher: SAGE Publications.

[40] Maeve Duggan. 2017. Online Harassment 2017. https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/

[41] Evelyne Durocher, Ryoa Chung, Christiane Rochon, and Matthew Hunt. 2016. Understanding and Addressing Vulnerability Following the 2010 Haiti Earthquake: Applying a Feminist Lens to Examine Perspectives of Haitian and Expatriate Health Care Providers and Decision-Makers. *Journal of Human Rights Practice* 8, 2 (July 2016), 219–238. https://doi.org/10.1093/jhuman/huw007

[42] Motahhare Eslami, Karrie Karahalios, Christian Sandvig, Kristen Vaccaro, Aimee Rickman, Kevin Hamilton, and Alex Kirlik. 2016. First I "like" it, then I hide it: Folk Theories of Social Feeds. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, San Jose California USA, 2371–2382. https://doi.org/10.1145/2858036.2858494

[43] Jessica L. Feuston and Anne Marie Piper. 2019. Everyday Experiences: Small Stories and Mental Illness on Instagram. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, Glasgow Scotland Uk, 1–14. https://doi.org/10.1145/3290605.3300495

[44] Jessica L. Feuston, Alex S. Taylor, and Anne Marie Piper. 2020. Conformity of Eating Disorders through Content Moderation. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW1 (May 2020), 040:1–040:28. https://doi.org/10.1145/3392845

[45] Ryan J. Gallagher, Elizabeth Stowell, Andrea G. Parker, and Brooke Foucault Welles. 2019. Reclaiming Stigmatized Narratives: The Networked Disclosure Landscape of #MeToo. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 1–30. https://doi.org/10.1145/3359198

[46] Aakash Gautam, Chandani Shrestha, Andrew Kulak, Steve Harrison, and Deborah Tatar. 2018. Participatory tensions in working with a vulnerable population. In *Proceedings of the 15th Participatory Design Conference: Short Papers, Situated Actions, Workshops and Tutorial - Volume 2 (PDC '18)*. Association for Computing Machinery, New York, NY, USA, 1–5. https://doi.org/10.1145/3210604.3210629

[47] Erinn Gilson. 2011. Vulnerability, Ignorance, and Oppression. *Hypatia* 26, 2 (2011), 308–332. https://doi.org/10.1111/j.1527-2001.2010.01158.x

[48] Barney G. Glaser and Ansel L. Strauss. 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research*.

[49] Oliver Haimson. 2018. Social Media as Social Transition Machinery. *Proceedings of the ACM on Human-Computer Interaction* 2 (Nov. 2018), 63. https://doi.org/10.1145/3274332

[50] Oliver L. Haimson, Justin Buss, Zu Weinger, Denny L. Starks, Dykee Gorrell, and Briar Sweetbriar Baron. 2020. Trans Time: Safety, Privacy, and Content Warnings on a Transgender-Specific Social Media Site. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (Oct. 2020), 124:1–124:27. https://doi.org/10.1145/3415195

[51] Oliver L. Haimson and Anna Lauren Hoffmann. 2016. Constructing and enforcing "authentic" identity online: Facebook, real names, and non-normative identities. *First Monday* (June 2016). https://doi.org/10.5210/fm.v21i6.6791

[52] Benjamin Hanckel, Son Vivienne, Paul Byron, Brady Robards, and Brendan Churchill. 2019. 'That's not necessarily for them': LGBTIQ+ young people, social media platform affordances and identity curation. *Media, Culture & Society* 41, 8 (Nov. 2019), 1261–1278. https://doi.org/10.1177/0163443719846612

[53] Eszter Hargittai. 2020. Potential Biases in Big Data: Omitted Voices on Social Media. *Social Science Computer Review* 38, 1 (Feb. 2020), 10–24. https://doi.org/10.1177/0894439318788322

[54] Eszter Hargittai and Eden Litt. 2011. The tweet smell of celebrity success: Explaining variation in Twitter adoption among a diverse group of young adults. *New Media & Society* 13, 5 (Aug. 2011), 824–842. https://doi.org/10.1177/1461444811405805

[55] Daniel Herron, Nazanin Andalibi, Oliver Haimson, Wendy Moncur, and Elise van den Hoven. 2016. HCI and Sensitive Life Experiences. In *Proceedings of the 9th Nordic Conference on Human-Computer Interaction (NordiCHI '16)*. Association for Computing Machinery, New York, NY, USA, 1–3. https://doi.org/10.1145/2971485.2987673

[56] 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*. ACM, Yokohama Japan, 1–18. https://doi.org/10.1145/3411764.3445778

[57] Sarah J. Jackson and Brooke Foucault Welles. 2015. Hijacking #MYNYPD: Social Media Dissent and Networked Counterpublics. *Journal of Communication* 65, 6 (Dec. 2015), 932–952. https://doi.org/10.1111/jcom.12185

[58] Samantha Jaroszewski, Danielle Lottridge, Oliver L. Haimson, and Katie Quehl. 2018. "Genderfluid" or "Attack Helicopter": Responsible HCI Research Practice with Non-binary Gender Variation in Online Communities. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, Montreal QC Canada, 1–15. https://doi.org/10.1145/3173574.3173881

[59] Jialun Aaron Jiang, Morgan Klaus Scheuerman, Casey Fiesler, and Jed R. Brubaker. 2021. Understanding international perceptions of the severity of harmful content online. *PLOS ONE* 16, 8 (Aug. 2021), e0256762. https://doi.org/10.1371/journal.pone.0256762

[60] Sanja Kapidzic and Susan C Herring. 2015. Race, gender, and self-presentation in teen profile photographs. *New Media & Society* 17, 6 (June 2015), 958–976. https://doi.org/10.1177/1461444813520301

[61] Nadia Karizat, Daniel Delmonaco, Motahhare Eslami, and Nazanin Andalibi. 2021. Algorithmic Folk Theories and Identity: How TikTok Users Co-Produce Knowledge of Identity and Engage in Algorithmic Resistance. (2021), 41.

[62] Dilara Kekulluoglu, Kami Vaniea, and Walid Magdy. 2022. Understanding Privacy Switching Behaviour on Twitter. In *CHI Conference on Human Factors in Computing Systems (CHI '22)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3491102.3517675

[63] Hanna Krasnova, Sarah Spiekermann, Ksenia Koroleva, and Thomas Hildebrand. 2010. Online Social Networks: Why We Disclose. *Journal of Information Technology* 25, 2 (June 2010), 109–125. https://doi.org/10.1057/jit.2010.6 Publisher: SAGE Publications Ltd.

[64] Neha Kumar and Naveena Karusala. 2021. Braving Citational Justice in Human-Computer Interaction. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, Yokohama Japan, 1–9. https://doi.org/10.1145/3411763.3450389

[65] Margaret Meek Lange, Wendy Rogers, and Susan Dodds. 2013. Vulnerability in Research Ethics: a Way Forward. *Bioethics* 27, 6 (2013), 333–340. https://doi.org/10.1111/bioe.12032 _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/bioe.12032.

[66] Caitlin E. Lawson. 2018. Platform vulnerabilities: harassment and misogynoir in the digital attack on Leslie Jones. *Information, Communication & Society* 21, 6 (June 2018), 818–833. https://doi.org/10.1080/1369118X.2018.1437203

[67] Alex Leavitt. 2015. "This is a Throwaway Account": Temporary Technical Identities and Perceptions of Anonymity in a Massive Online Community. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '15)*. Association for Computing Machinery, New York, NY, USA, 317–327. https://doi.org/10.1145/2675133.2675175

[68] Jioni A. Lewis, Ruby Mendenhall, Stacy A. Harwood, and Margaret Browne Huntt. 2016. "Ain't I a Woman?": Perceived Gendered Racial Microaggressions Experienced by Black Women. *The Counseling Psychologist* 44, 5 (July 2016), 758–780. https://doi.org/10.1177/0011000016641193

[69] Eden Litt. 2012. Knock, Knock. Who's There? The Imagined Audience. *Journal of Broadcasting & Electronic Media* 56, 3 (July 2012), 330–345. https://doi.org/10.1080/08838151.2012.705195 Publisher: Routledge _eprint: https://doi.org/10.1080/08838151.2012.705195.

[70] Catriona Mackenzie, Wendy Rogers, and Susan Dodds (Eds.). 2013. *Vulnerability: new essays in ethics and feminist philosophy*. Oxford University Press, New York.

[71] Alice E. Marwick and danah boyd. 2011. I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society* 13, 1 (Feb. 2011), 114–133. https://doi.org/10.1177/1461444810365313 Publisher: SAGE Publications.

[72] Alice E. Marwick and danah boyd. 2014. Networked privacy: How teenagers negotiate context in social media. *New Media & Society* 16, 7 (Nov. 2014), 1051–1067. https://doi.org/10.1177/1461444814543995

[73] Nora McDonald, Karla Badillo-Urquiola, Morgan G. Ames, Nicola Dell, Elizabeth Keneski, Manya Sleeper, and Pamela J. Wisniewski. 2020. Privacy and Power: Acknowledging the Importance of Privacy Research and Design for Vulnerable Populations. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI EA '20)*. Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/3334480.3375174

[74] Nora McDonald and Andrea Forte. 2020. The Politics of Privacy Theories: Moving from Norms to Vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Honolulu HI USA, 1–14. https://doi.org/10.1145/3313831.3376167

[75] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 1–23. https://doi.org/10.1145/3359174

[76] Matthew B. Miles and A. Michael Huberman. 1994. *Qualitative data analysis: An expanded sourcebook, 2nd ed.* Sage Publications, Inc, Thousand Oaks, CA, US. Pages: xiv, 338.

[77] Cosmin Munteanu, Heather Molyneaux, and Susan O'Donnell. 2014. Fieldwork with vulnerable populations. *Interactions* 21, 1 (Jan. 2014), 50–53. https://doi.org/10.1145/2543579

[78] John A. Naslund and Kelly A. Aschbrenner. 2019. Risks to Privacy With Use of Social Media: Understanding the Views of Social Media Users With Serious Mental Illness. *Psychiatric Services* 70, 7 (July 2019), 561–568. https://doi.org/10.1176/appi.ps.201800520 Publisher: American Psychiatric Publishing.

[79] Robert C Nickerson, Upkar Varshney, and Jan Muntermann. 2013. A method for taxonomy development and its application in information systems. *European Journal of Information Systems* 22, 3 (May 2013), 336–359. https://doi.org/10.1057/ejis.2012.26

[80] Julia Omarzu. 2000. A Disclosure Decision Model: Determining How and When Individuals Will Self-Disclose. *Personality and Social Psychology Review* 4, 2 (May 2000), 174–185. https://doi.org/10.1207/S15327957PSPR0402_05 Publisher: SAGE Publications Inc.

[81] Patrick B O'Sullivan and Caleb T Carr. 2018. Masspersonal communication: A model bridging the mass-interpersonal divide. *New Media & Society* 20, 3 (March 2018), 1161–1180. https://doi.org/10.1177/1461444816686104

[82] Leysia Palen and Paul Dourish. 2003. Unpacking "privacy" for a networked world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '03)*. Association for Computing Machinery, New York, NY, USA, 129–136. https://doi.org/10.1145/642611.642635

[83] Michael Quinn Patton. 2015. *Qualitative research & evaluation methods: integrating theory and practice* (fourth edition ed.). SAGE Publications, Inc, Thousand Oaks, California.

[84] Katy E. Pearce, Jessica Vitak, and Kristen Barta. 2018. Privacy at the Margins| Socially Mediated Visibility: Friendship and Dissent in Authoritarian Azerbaijan. *International Journal of Communication* 12, 0 (March 2018), 22. https://ijoc.org/index.php/ijoc/article/view/7039 Number: 0.

[85] James W. Pennebaker. 1997. *Opening Up: The Healing Power of Expressing Emotions*. Guilford Press. Google-Books-ID: F3gF8OoKydQC.

[86] Danielle Petherbridge. 2016. What's Critical about Vulnerability? Rethinking Interdependence, Recognition, and Power. *Hypatia* 31, 3 (2016), 589–604. https://doi.org/10.1111/hypa.12250

[87] Sandra Petronio. 2002. *Boundaries of Privacy: Dialectics of Disclosure*. SUNY Press. Google-Books-ID: gTCsft8zVXgC.

[88] James Pierce, Sarah Fox, Nick Merrill, and Richmond Wong. 2018. Differential Vulnerabilities and a Diversity of Tactics: What Toolkits Teach Us about Cybersecurity. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (Nov. 2018), 139:1–139:24. https://doi.org/10.1145/3274408

[89] Anthony T. Pinter, Jialun Aaron Jiang, Katie Z. Gach, Melanie M. Sidwell, James E. Dykes, and Jed R. Brubaker. 2019. "Am I Never Going to Be Free of All This Crap?": Upsetting Encounters with Algorithmically Curated Content About Ex-Partners. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 1–23. https://doi.org/10.1145/3359172

[90] Anastasia Powell. 2015. Seeking rape justice: Formal and informal responses to sexual violence through technosocial counter-publics. *Theoretical Criminology* 19, 4 (Nov. 2015), 571–588. https://doi.org/10.1177/1362480615576271

[91] Anastasia Powell, Adrian J Scott, and Nicola Henry. 2020. Digital harassment and abuse: Experiences of sexuality and gender minority adults. *European Journal of Criminology* 17, 2 (March 2020), 199–223. https://doi.org/10.1177/1477370818788006

[92] Cassidy Pyle, Lee Roosevelt, Ashley Lacombe-Duncan, and Nazanin Andalibi. 2021. LGBTQ Persons' Pregnancy Loss Disclosures to Known Ties on Social Media: Disclosure Decisions and Ideal Disclosure Environments. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, Yokohama Japan, 1–17. https://doi.org/10.1145/3411764.3445331

[93] Wendy Rogers, Catriona Mackenzie, and Susan Dodds. 2012. Why bioethics needs a concept of vulnerability. *IJFAB: International Journal of Feminist Approaches to Bioethics* 5, 2 (Sept. 2012), 11–38. https://doi.org/10.3138/ijfab.5.2.11

[94] Aja Romano. 2018. YouTube's PewDiePie amplified anti-Semitic rhetoric. Again. *Vox* (Dec. 2018). https://www.vox.com/2018/12/13/18136253/pewdiepie-vs-tseries-links-to-white-supremacist-alt-right-redpill

[95] Johnny Saldaña. 2014. Coding and Analysis Strategies. In *The Oxford Handbook of Qualitative Research*, Patricia Leavy (Ed.). Oxford University Press, 580–598. https://doi.org/10.1093/oxfordhb/9780199811755.013.001

[96] Michael Salter. 2013. Justice and revenge in online counter-publics: Emerging responses to sexual violence in the age of social media. *Crime, Media, Culture: An International Journal* 9, 3 (Dec. 2013), 225–242. https://doi.org/10.1177/1741659013493918

[97] Morgan Klaus Scheuerman, Aaron Jiang, Katta Spiel, and Jed R. Brubaker. 2021. Revisiting Gendered Web Forms: An Evaluation of Gender Inputs with (Non-)Binary People. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, Yokohama Japan, 1–18. https://doi.org/10.1145/3411764.3445742

[98] Morgan Klaus Scheuerman, Jialun Aaron Jiang, Casey Fiesler, and Jed R. Brubaker. 2021. A Framework of Severity for Harmful Content Online. *arXiv:2108.04401 [cs]* (Aug. 2021). https://doi.org/10.1145/3479512 arXiv: 2108.04401.

[99] Ari Schlesinger, W. Keith Edwards, and Rebecca E. Grinter. 2017. Intersectional HCI: Engaging Identity through Gender, Race, and Class. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, Denver Colorado USA, 5412–5427. https://doi.org/10.1145/3025453.3025766

[100] Sarita Schoenebeck and Lindsay Blackwell. 2021. Reimagining Social Media Governance: Harm, Accountability, and Repair. *SSRN Electronic Journal* (2021). https://doi.org/10.2139/ssrn.3895779

[101] Sarita Schoenebeck, Oliver L Haimson, and Lisa Nakamura. 2021. Drawing from justice theories to support targets of online harassment. *New Media & Society* 23, 5 (May 2021), 1278–1300. https://doi.org/10.1177/1461444820913122

[102] Andi Schwartz. 2020. Radical vulnerability: selfies as a Femme-inine mode of resistance. *Psychology & Sexuality* (Aug. 2020), 1–14. https://doi.org/10.1080/19419899.2020.1810745

[103] Bryan Semaan, Lauren M. Britton, and Bryan Dosono. 2017. Military Masculinity and the Travails of Transitioning: Disclosure in Social Media. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*. ACM, Portland Oregon USA, 387–403. https://doi.org/10.1145/2998181.2998221

[104] Elisabeth Sheff. 2014. *The polyamorists next door: inside multiple-partner relationships and families*. Rowman & Littlefield Publishers, Inc, Lanham.

[105] William B. Stiles. 1987. "I Have to Talk to Somebody". In *Self-Disclosure: Theory, Research, and Therapy*, Valerian J. Derlega and John H. Berg (Eds.). Springer US, Boston, MA, 257–282. https://doi.org/10.1007/978-1-4899-3523-6_12

[106] Elizabeth Stowell, Mercedes C. Lyson, Herman Saksono, Reneé C. Wurth, Holly Jimison, Misha Pavel, and Andrea G. Parker. 2018. Designing and Evaluating mHealth Interventions for Vulnerable Populations: A Systematic Review. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–17. http://doi.org/10.1145/3173574.3173589

[107] Jeffrey W. Treem and Paul M. Leonardi. 2013. Social Media Use in Organizations: Exploring the Affordances of Visibility, Editability, Persistence, and Association. *Annals of the International Communication Association* 36, 1 (Jan. 2013), 143–189. https://doi.org/10.1080/23808985.2013.11679130 Publisher: Routledge _eprint: https://doi.org/10.1080/23808985.2013.11679130.

[108] Jeffrey W. Treem, Paul M. Leonardi, and Bart van den Hooff. 2020. Computer-Mediated Communication in the Age of Communication Visibility. *Journal of Computer-Mediated Communication* 25, 1 (March 2020), 44–59. https://doi.org/10.1093/jcmc/zmz024

[109] Anthony Henry Triggs, Kristian Møller, and Christina Neumayer. 2021. Context collapse and anonymity among queer Reddit users. *New Media & Society* 23, 1 (Jan. 2021), 5–21. https://doi.org/10.1177/1461444819890353 Publisher: SAGE Publications.

[110] Zeynep Tufekci. 2017. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. Yale University Press. Google-Books-ID: x7S_DgAAQBAJ.

[111] Tanvir C Turin, Tasnima Abedin, Nashit Chowdhury, Mahzabin Ferdous, Marcus Vaska, Nahid Rumana, Rossana Urrutia, and Mohammad Ziaul Islam Chowdhury. 2020. Community engagement with immigrant communities involving health and wellness research: a systematic review protocol towards developing a taxonomy of community engagement definitions, frameworks, and methods. *BMJ Open* 10, 4 (April 2020), e035649. https://doi.org/10.1136/bmjopen-2019-035649

[112] John Vines, Roisin McNaney, Rachel Clarke, Stephen Lindsay, John McCarthy, Steve Howard, Mario Romero, and Jayne Wallace. 2013. Designing for- and with- vulnerable people. In *CHI '13 Extended Abstracts on Human Factors in Computing Systems (CHI EA '13)*. Association for Computing Machinery, New York, NY, USA, 3231–3234. https://doi.org/10.1145/2468356.2479654

[113] Jessica Vitak, Katie Shilton, and Zahra Ashktorab. 2016. Beyond the Belmont Principles: Ethical Challenges, Practices, and Beliefs in the Online Data Research Community. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*. ACM, San Francisco California USA, 941–953. https://doi.org/10.1145/2818048.2820078

[114] Ashley Marie Walker and Michael A. DeVito. 2020. "'More gay' fits in better": Intracommunity Power Dynamics and Harms in Online LGBTQ+ Spaces. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Honolulu HI USA, 1–15. https://doi.org/10.1145/3313831.3376497

[115] Tao Wang, Monica Garfield, Pamela Wisniewski, and Xinru Page. 2020. Benefits and Challenges for Social Media Users on the Autism Spectrum. In *Conference Companion Publication of the 2020 on Computer Supported Cooperative Work and Social Computing*. Association for Computing Machinery, New York, NY, USA, 419–424. https://doi.org/10.1145/3406865.3418322

[116] Renwen Zhang, Natalya N. Bazarova, and Madhu Reddy. 2021. Distress Disclosure across Social Media Platforms during the COVID-19 Pandemic: Untangling the Effects of Platforms, Affordances, and Audiences. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–15. http://doi.org/10.1145/3411764.3445134

[117] Xuan Zhao, Cliff Lampe, and Nicole B. Ellison. 2016. The Social Media Ecology: User Perceptions, Strategies and Challenges. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, San Jose California USA, 89–100. https://doi.org/10.1145/2858036.2858333

Received January 2022; revised July 2022; accepted November 2022