Accounting for Privacy Pluralism: Lessons and Strategies from Community-Based Privacy Groups

Erica Shusas
ejr93@drexel.edu
Drexel University
Philadelphia, PA, USA

Patrick Skeba
pts217@lehigh.edu
Lehigh University
Bethlehem, PA, USA

Eric P. S. Baumer
ericpsb@lehigh.edu
Lehigh University
Bethlehem, PA, USA

Andrea Forte
aforte@drexel.edu
Drexel University
Philadelphia, PA, USA

ABSTRACT

The emergent, dynamic nature of privacy concerns in a shifting sociotechnical landscape creates a constant need for privacy-related resources and education. One response to this need is community-based privacy groups. We studied privacy groups that host meetings in diverse urban communities and interviewed the meeting organizers to see how they grapple with potentially varied and changeable privacy concerns. Our analysis identified three features of how privacy groups are organized to serve diverse constituencies: situating (finding the right venue for meetings), structuring (finding the right format/content for the meeting), and providing support (offering varied dimensions of assistance). We use these findings to inform a discussion of "privacy pluralism" as a perennial challenge for the HCI privacy research community, and we use the practices of privacy groups as an anchor for reflection on research practices.

CCS CONCEPTS

• **Human-centered computing, Empirical studies in collaborative and social computing**;

KEYWORDS

privacy, meetup, privacy groups, community organizations, privacy resources, privacy pluralism

ACM Reference Format:
Erica Shusas, Patrick Skeba, Eric P. S. Baumer, and Andrea Forte. 2023. Accounting for Privacy Pluralism: Lessons and Strategies from Community-Based Privacy Groups. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23), April 23–28, 2023, Hamburg, Germany*. ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3544548.3581331

CHI '23, April 23–28, 2023, Hamburg, Germany

ACM ISBN 978-1-4503-9421-5/23/04…$15.00
https://doi.org/10.1145/3544548.3581331

1 INTRODUCTION

> *"Privacy is not one thing, but many distinct but related things. For too long, policymakers and others have viewed privacy too myopically and narrowly, failing to recognize many important privacy problems. Understanding privacy in a more pluralistic manner will hopefully improve the way privacy problems are recognized and addressed." - Daniel Solove [65, p. 78]*

Privacy is recognized as a fundamental human right [6]. While there is consensus on the importance of privacy and of helping people obtain it, there is less consensus on what exactly "it" is that people seek to obtain. Privacy researchers and scholars offer widely varying conceptualizations, from "the right to be le[f]t alone" [70, p. 193], to informational boundary regulation [51–53], to contextual constrains on acceptable flows of information [49, 50], to a qualitative measure of the difficulty or "friction" involved in obtaining certain information [21, 63].

Moreover, individual technology users often vary greatly in their privacy concerns and experiences. What counts as a privacy concern can differ depending on gender [4, 39], age [11], religion [1], socioeconomic status [18], education level [11], cultural background [1, 5, 32], and many other factors. At times, different people even have different underlying conceptualizations about what the concept privacy is [73]. Furthermore, novel sociotechnical arrangements—from social media [12], to mobile phones [4], to inferential algorithms [63]—often precipitate emergent and difficult to predict privacy concerns. These novel concerns then require people to seek out information and advice from a variety of sources. For example, some people seek support from social media platforms such as Reddit [38] and other online resources [55], while others obtain guidance from educational institutions [55] or from family and friends [37].

To seek advice about their complex, nuanced individual privacy concerns, some people consult self-organized privacy groups. These often community-based groups attempt to serve constituencies that are diverse (in terms of demographics, technology familiarity, education level, etc.) and that have widely varying privacy concerns. Thus, these groups must be organized in ways that cater to and address a plurality of different privacy concerns. In some ways, the job of these group organizers resembles that of HCI researchers, for whom coping with the radical variety of differences in human

experiences is a perennial challenge. How are privacy groups organized that enable them to serve diverse populations and their privacy concerns more pluralistically?

To explore this question, we conducted fieldwork with three different groups, each of which aspired to serve potentially diverse constituencies with widely varying privacy concerns and practices. Our work involved attending 13 individual meetings of these groups, as well as single meetings of a variety of other related or similar groups, and conducting interviews with 6 organizers of privacy meetup[1] groups in large urban areas. Given the diversity of constituencies each group aimed to serve, we sought to learn from privacy group organizers about how they conceive of their audiences and how they organize their groups and events in response to this diversity. We propose that insights from these organizers can provide guidance or inspiration for how we, as researchers, might similarly account for privacy pluralism in our work.

Our analysis suggests three specific characteristics of how these groups were organized that allowed them to meet the needs of diverse people with interests in, experiences of, and concerns about privacy: First, *situating* meetings in person and in public was regarded as an important way of both protecting and engaging participants. Second, *structuring* the meetings so that the content discussed was guided by the participants allowed organizers to acknowledge that the attendees have sources of threat, issues of interest, and preferred learning strategies that are unique and may differ from those of the organizers. Finally, we observed the groups *supporting* members and attendees in multiple ways, including informational, emotional, and other types of support.

We suggest that the combination of these characteristics helps achieve what we term *privacy pluralism*, an orientation that resonates with the foundational work of Daniel Solove who called for "understanding privacy in a more pluralistic manner" [65, p. 78] to account for and respect the coexistence of multiple, divergent privacy concerns, experiences, and practices. In our analysis, we observed how privacy pluralism extends beyond a way of understanding privacy to encompass real world enactments and actions. After describing the three characteristics of privacy groups in detail, we conclude by suggesting strategies inspired by each of these characteristics that privacy researchers and designers could employ to better enact privacy pluralism.

2 RELATED WORK

HCI literature is rich with studies demonstrating that privacy concerns are socially and culturally contingent [1, 2, 58]. Social factors such as gender dynamics and inequities [4], adherence to religious principles [1], and generational differences [27] or age [45] have all been found to influence privacy practices and concerns. People with marginalized identity features in particular have been found to experience unique privacy threats [42] and to have a variety of responses to threats that themselves carry different types of risk [59]. A comprehensive review of such studies could fill more than one paper but even this small selection offers a glimpse of the empirical evidence that buttresses Solove's call for a pluralistic understanding of privacy. The question remains, what kinds of responses might a community of scholars have to this radical divergence in experiences of privacy?

Some responses have been technical. Prior research on design has sought to address the challenges of creating technologies that support the privacy needs of particular populations. For example, to address the disproportionate amount of institutional surveillance marginalized populations encounter on centralized online social networks (cOSNs) such as Facebook and Instagram, Logas et al. suggested decentralized privacy overlays (DePOs), which allow users to selectively share content on cOSNs through decentralized content distribution networks [41]. Other examples include Silva et al.'s recommendation for user evaluations of privacy settings in consideration of younger age groups who are particularly vulnerable to usability challenges [62] and Afnan et al.'s suggestion of identity-based audience controls and cross-platform data management to contend with context collapse, inspired by the privacy challenges experienced by Muslim-American women [2]. In reviewing literature on privacy and marginalization, Sannon and Forte identified four approaches to technological interventions that support privacy needs of specific groups: providing greater control over information, facilitating management of communal privacy, making privacy easier, and building technical safeguards [59]. Wong and Mulligan offer an overview of Privacy by Design literature and observe that "privacy and design work in HCI is heavily weighted towards design to solve a privacy problem or to inform and support privacy" [74], underscoring that design responses to the diversity of privacy experiences tend to be informed by concern for the requirements of specific groups and suggesting concrete innovative ways that HCI and design can play a role in privacy futures.

Other responses to the diversity of privacy experiences have been broad and conceptual. For example, Nissenbaum's *contextual integrity* [48] was highlighted by Barkhuus as an important instrument for the HCI community in that it offers a conceptual framework within which HCI researchers can investigate the privacy expectations and norms of a particular social context [7]. More recently, McDonald and Forte argued that norm-based privacy theories may overlook the behaviors and motivations of individuals who do not maintain a dominant social status and suggest the notion of *privacy vulnerability* as a corrective measure [44] to take into account power relationships even within subpopulations and communities. Writing for a Communication audience, Reichel goes further to suggest that the very discourse of privacy is problematic in that it works to reproduce technical structures that marginalize certain groups and should be replaced with the concept of dignity [56].

Many scholars have argued for privacy to be conceived of as essentially contested, that is, malleable across contexts and sociotechnical arrangements [47]. However, the corollary of dynamic and diverse privacy conceptualizations is the pragmatic challenges that this brings to privacy researchers, designers, and policy makers [23, 47, 64, 65]. Whereas many technical/design approaches to privacy investigate a specific "user group" to understand their needs and challenges in service of designing technical arrangements that support them, and whereas many conceptual approaches to privacy delicately articulate important ways of thinking that refine our theoretical understandings of the space, in this work, we aim to understand privacy pluralism as a particular form of action. How is

[1]The term "meetup" here refers to the generic practice of social events organized around a theme or interest, rather than the event-based social media platform meetup.com.

privacy pluralism as a way of thinking enacted in the world? In the "wild?" In answering these questions, we aim to develop pragmatic insights for designers and researchers who embrace a pluralistic approach to privacy.

3 METHOD

We conducted a qualitative study of privacy groups that convened in person in urban East Coast areas of the US as well as online. Specifically, we used ethnographic methods, including participant observation and semi-structured interviews, to investigate how organizers of privacy groups that are open to all members of the public manage the diverse privacy issues, needs, and understandings that participants bring. We analyzed the data using iterative inductive methods and present and discuss findings with the goal of transferability—a characteristic of qualitative research that allows readers to apply what is learned to contexts outside the original study. This is generally accomplished through connections to other work and thick description [40].

3.1 Site Selection and Recruitment

We identified privacy groups by searching general event listing websites and online privacy-oriented resources, as well as in-person community boards in public gathering places such as libraries and bookstores. The author attended privacy group meetings from January 2020 through September 2021. Unsurprisingly, the privacy groups we discovered had a range of objectives, from large networking events for privacy professionals to small gatherings of skilled hobbyists focused on collaborating on privacy-enhancing projects. A few of the privacy group events were oriented towards a broader audience that we felt would better address our research question. After considering several possible groups for further data collection, we identified three groups, all of whom sought to serve diverse populations with varying privacy concerns. The first of these groups is a privacy collective that organized in response to the many privacy concerns that the general public may have related to digital technologies. The second group is a non-profit that works with communities that are prone to surveillance, particularly communities of color, women, and the LGBTQ+ communities. The third group is comprised of women in technology who host open meetings on multiple subjects including topics related to online privacy.

The first author attended six in-person meetings of the first organization. Five of the in-person meetings were dedicated to a privacy topic (three at a bookstore, two at a public library), and one in-person meeting was an event open to the public in which upcoming events, fundraising, and other administrative matters were discussed. After the onset of the pandemic, the first author attended four online events hosted by the same organization. Furthermore, the first author attended two online events hosted by the second organization and one online event hosted by the third organization that were each devoted to a privacy topic. The first author's attendance at the privacy group meetings helped identify organizers to potentially interview, as well as gain insight into how the meetings were run firsthand and corroborate interview data. We then recruited group organizers for interviews to understand their strategies and challenges in organizing privacy meetups and how they thought about the diverse constituencies they serve. Interview participants were recruited directly via contacts made at meetups and using online contact information and through snowball sampling.

3.2 Data Collection

Field notes were taken at the in-person and online privacy group meetings. The first author disclosed herself as a researcher to the privacy group meeting hosts and maintained a role of participant observer at the meetings. Interviews were conducted between November 2020 and September 2021. Initially, data collection was planned in person for spring and summer of 2020; when the pandemic struck, we postponed data collection, but it soon became clear that in-person data collection would not be possible. Moreover, we viewed the shift of operations from in person to online meetings as an opportunity for participants to reflect on their events and identify important features of organizing. The first author attended ten meetings of the first group, two meetings of the second group, and one of the third.

The first author conducted six interviews with individuals involved in organizing all three privacy groups. Our first three interview participants (P1, P2, P3) were from the first organization (the privacy collective). As the interviews proceeded, the first author discussed emergent themes and insights with the rest of the group. Once we determined that we were hearing consistent themes from these participants, an additional two participants (P4, P5) were recruited from the second group (the non-profit), and one participant (P6) from the third (the group of women in technology). The additional three interviews largely reinforced themes introduced in the initial three interviews and so we considered this to be sufficient for data saturation and concluded data collection.

Organizers who volunteered to participate in interviews were offered the choice of being interviewed over Zoom, by phone, or to suggest a means of communication that was more aligned with their personal privacy preferences. Ultimately, five interviews took place over Zoom and were audio recorded and one took place over the phone while the interviewer took notes. All three groups were active prior to the pandemic and remained active throughout data collection. Interviews lasted 30-60 minutes, and participants were offered $25 in cash or an Amazon gift card for their time.

3.3 Qualitative Analysis

The interview data were transcribed using the service Rev.com and analyzed using an inductive thematic analysis approach [10]. After familiarization with the transcripts, the first author performed line-by-line iterative, inductive coding of all the interviews which produced a set of open codes. The open codes were collated into potential themes and reviewed with the research team who met regularly to discuss patterns in the data as iterative analysis continued. The group collaboratively constructed a shared interpretation of the findings through discussion as well as iterative writing, rewriting, and restructuring of findings.

3.4 Fieldsites

A primary objective stated by several privacy group organizers was the curation of a safe-feeling space for their meetings. The

organizers agreed to have a researcher present at meetings, but it was requested that no data would be reported about the attendees or any members of the group who had not explicitly agreed to participate in the study. Therefore, in lieu of providing a thick description of an actual privacy meetup that would compromise our agreement with organizers, we present the following first-person composite vignette of a privacy meetup that is constructed from the real experiences of the first author.

> *A bell jangled as I pushed through the door out of the cold and gray winter day into the confined but cozy bookshop. I scanned the crowd and was at first unable to discern the bookshop's potential clientele from the privacy group attendees. I saw a small assemblage gathered in chairs in the corner and made my way over to them. Before I could ask if they were the group I was looking for, one of the seated individuals who had a clipboard in hand introduced themselves as a representative of the privacy group and warmly encouraged me to grab a chair. After some small talk and as a few more additional attendees filtered in, the same group member who had just introduced themselves to me moments before announced that the meeting was beginning and introduced herself as the host. She shared that the topic of the meeting was privacy practices on the job and some guidelines for participation, emphasizing the use of respectful language towards one another. Everyone was encouraged to ask questions, share experiences, offer advice, or just listen.*
>
> *One group member began with a short talk on some general practices that might enhance one's privacy while at work and offered some strengths and weaknesses of each strategy. Then the host opened the discussion to the attendees. One attendee shared how she had worked hard to minimize the amount of personal information she shared online, and was deeply troubled that her employer was now requiring all employees to use Google Docs. Another woman in the group shared a similar experience and how she was able to advocate for herself to her boss who eventually allowed her to use a different platform. Another attendee then disclosed that he worked from home and was fairly confident that his hardware was secure, but he wondered if anyone had any advice on how to make his internet connections more secure. An attendee who introduced herself as an IT worker gave him some advice on user-friendly VPNs. Yet another attendee spoke up and said that it was a little off-topic, but he had been disheartened lately at all the pressure he was getting from friends and family to rejoin social media. Several of the group members commiserated with him.*
>
> *After two hours of continuous back-and-forth and discussion, the meeting ended with the host sharing a few more upcoming events and some recommendations of resources they trusted for information on privacy. As the meeting ended, participants dispersed, some retreating into the bookstore's aisles while I, along with a few others, hustled back out the front door into the bleak and biting air.*

This vignette is based on the first author's field notes with altered details and provides readers with a sense of what the in-person privacy meetups were like. The move to primarily online interactions after the onset of the COVID-19 pandemic saw interesting deviations from this structure. Online meetings had various arrangements and used technology differently to create different kinds of meeting places. Overall, organizers communicated their struggles in finding acceptable remote relocations, and several setups were tried. For example, some organizers arranged for meetings to take place on online communication platforms hosted by larger partner organizations, while other organizers experimented with platforms that allowed for greater anonymity for participants. Although there were varying degrees of satisfaction with the remote meetings, most organizers conveyed that they were looking forward to the return of in-person events.

3.5 Ethical Considerations

As with any research, we took pains to ensure our data collection, analysis, and reporting in no way created privacy or other vulnerabilities for participants. Several of the participants were not comfortable sharing their demographic information so we do not report it. We modified any potentially identifying passages when reporting verbatim quotes and we refrained from reporting demographic characteristics of participants because several of them cited concerns in providing potentially identifiable personal information. The research was designated exempt by our institutional IRBs and we amended our in-person protocols to include online participation and data collection at the onset of the pandemic.

4 FINDINGS

Our analysis identified three key practices of privacy group organizers that explain how they serve pluralistic privacy concerns among their diverse constituencies.

- **Situating**. Organizers paid careful attention to engineering the environment in which interactions took place. Our participants emphasized that for these groups, holding meetings in public and in person was essential to assure and engage diverse participants.
- **Structuring**. Organizers considered how to format their events to better connect with their heterogeneous audience, underscoring their attempts to allow the content to be guided by participants in an effort to address pluralistic privacy concerns.
- **Supporting**. Organizers adopted a broad understanding of support, describing many different dimensions of assistance that meetings offer participants as fundamental to supporting people working through unique privacy concerns.

4.1 Situating: in Person and in Public

Privacy group organizers reported that they gave careful consideration to the context in which their meetings were situated. Situating meetings meant creating an environment that achieved several things: trust/safety among members, transparency, and visibility/accessibility to a wide range of attendees. A strong crosscutting theme across organizers' experiences related to all of these goals was the importance of their events being open and accessible to the public. Although the practice of meeting in public might seem at odds with the objective of discussing privacy issues, the privacy group organizers provided several reasons for why situating the meetings in person, and often in public, was important to connect with their desired audience.

Situating for Trust and Safety. Some of the people the organizers were interested in connecting with were from vulnerable communities who might feel more comfortable approaching the group if the meetings were held out in the open and in not only neutral but safe feeling spaces. One organizer stated:

> "Considering the spaces that we were trying to be at whether it was, you know, The Venue, or more directly like Fogwilde Bookstore, which is a feminist bookstore, I think dealing with folks in communities who have historically seen a lot of violence done to them whether online or in person, but certainly [online]. It was always important for us to be accessible so that folks feel comfortable approaching us to talk about these issues, even if they don't tell us everything about their situation because they might not feel comfortable doing so." (P2)

A second reason for situating for trust was that sensitive topics that might be more easily discussed if a degree of trust is established. Having repeated in-person meetings where attendees could return and see the same group members present helped foster that trust. One participant explained that having "regulars" who got to know people's names was important:

> "I think that was really, I think that was really useful because we were talking about privacy and sensitive topics and all of it sounds a little bit of conspiratorial. Having actual trust in knowing people is an important step in that, because some of the things we know to be true sound a little crazy." (P3)

Situating meetings in person not only helped to establish trust among attendees, but also addressed distrust of technologies. Distrust of particular technologies may have motivated attendees to seek our privacy groups in the first place. In-person meetings provide a kind of safe respite from a world of surveillance capitalism [76]. One organizer explained:

> "Yeah, people just want to learn more and more. They've heard a lot of things and they want to just talk to someone in person, especially if there's someone that doesn't necessarily trust the internet." (P2)

Situating for Transparency. Another strategy to engender trust was by situating events that encouraged a certain degree of transparency about how the group itself operated. One participant from the privacy collective described how they routinely held group administrative meetings that were open to the public:

> "[...] just kind of open once a month open meeting where folks who want to take part in the work or want to learn more about the work that we do can just kind of come by and see how we make decisions and and do stuff. So I think transparency has always been a central part of what what we do and building trust in the folks that we work with." (P2)

Situating for Visibility and Accessibility. Privacy group organizers also situated their meetings in public spaces to increase visibility to people who might otherwise not know about the existence of such groups or not be regular participants in privacy conversations. Accessibility to diverse audiences surfaced again and again in different ways. One organizer asserted that holding events in public places helped expose their organization to people who might otherwise be unaware that privacy groups such as theirs existed:

> "With a group that's new like us and a topic that's not as readily in the mainstream always, I think, doing the work in public spaces is important for us because it allows us [to] catch the attention of people who may not, who may not already be like plugged in." (P4)

Another organizer expressed that staging public events helped curate a sense of openness to newcomers:

> "We just wanted to be open [and] accessible to as many people as possible. So the our events being public was important because we didn't want to, [a]s much as we wanted to create a community and we want to wanted to have folks come through and feel comfortable, we didn't want to create like a bubble. We wanted to always be open to new folks." (P2)

Yet another organizer stressed the desire to maintain a low barrier to entry to their events, which included ensuring that cost was not a prohibitive factor:

> "We wanted to have the barrier to having people come to us be as low as possible, which included like we had some offers by places to come do workshops and they said, we'll, we'll have to charge like a ticket entry fee. And we were like, no, we won't do that." (P1)

A few of the organizers stipulated that by situating the meetings in person, those in attendance with more technical skill could work directly with those who were having issues or questions about their devices or would benefit from hands on instruction, creating a community approach to education. One interview participant stated situating meetings in person also helped make the meetings accessible to attendees without a lot of technical skills or experience and who might not be proficient or comfortable with video conferencing tools:

> "An open public space, I think, is really, really kind of critical on which leads into the code stuff we can't do that, and so the main outreach and educational nectar is closed. And I don't think since since that people we're trying to reach are [...] not technical, I don't think Zoom calls would be worthwhile." (P3)

Situating During Lockdowns. The importance of public, in-person meetings may have been accentuated by participants' recent (at the time of the interviews) pivot to online, remote formats due to the COVID-19 pandemic. We observed that organizers spent a great deal of time carefully considering how to situate online events during the transition. The first author began attending in-person privacy group meetings a few months before the onset of the pandemic, continued attending meetings after the transition to online, and observed as group members navigated extensive discussions about what online platforms were sufficiently privacy friendly and would foster a feeling of safety and trust for remote participants. Making online events accessible was seen as important given the new environment people were navigating during quarantine. Several of the organizers stated that they struggled to find an online platform that they felt confident would provide sufficient security for their attendees.

> "I think, I think we've thought about this a lot and in trying to make ourselves as accessible as possible, especially now during quarantine, [as] accessible and available to folks who need information as possible." (P2)

Overall, there was a strong trend in the data toward valuing in-person public events over any of the solutions that were ultimately tried in online platforms.

4.2 Structuring: Letting Attendees Lead

A crosscutting theme throughout the interviews was that, ideally, events should be structured to surface and address privacy concerns of attendees. Goals for structuring according to attendees' needs included serving diverse attendees' needs and helping people think critically and make informed choices about privacy. This flexible approach to structuring was frequently contrasted with typical cybersecurity trainings or "CryptoParty" events where people share knowledge about how to protect oneself in digital spaces [72], which was described as hierarchical and tool-centered. A common description of a CryptoParty event involved individuals with technical expertise teaching attendees how to use a specific tool that was presumed to make them all safer. However, the participants who had experienced these meetings found that there was often a disconnect between the varied needs of the individuals they had interacted with and the universal solutions beings taught in other cybersecurity meetings.

Structuring to Meet Diverse Needs. Participants explained that their groups served people with diverse understandings and experiences of privacy and that a universal approach would fail to serve these diverse needs. One organizer explained the structure of the events as predicated on respect for attendees' experiences and understandings of what threats they face:

> "Especially considering especially that we were going into a lot of different spaces and community spaces. We never wanted to tell people what's their threat models [...] we just start with the assumption that people know what their threat models are and we're just providing resources and suggestions. So we never really wanted to feel like this group or force that came into a situation [that] was like this [is] what you have to do." (P2)

Individual attendees' backgrounds and identities played a strong role in organizers' explanations of why structuring to support diverse privacy concerns was important. P5 stated that common themes like keeping one's self safe were "very different if you're talking to a group of protesters" compared with people who were "just focused on what can I do for myself? What can I do for my family?" These different goals might stem from different activities and situations, but might also stem from identity characteristics like belonging to a marginalized group.

A few of the participants shared that their interest in privacy issues stemmed from their own or an acquaintance's experiences with targeted surveillance. P6 became interested in privacy issues after learning from a teacher who was a black Muslim about being a target of surveillance as a minority. P4 became interested in privacy issues because of his own experiences being a target of surveillance as a minority, and shared his thoughts on how unequal power structures impact the options available for some groups disproportionately:

> "Is privacy equal for everyone? I think now, and I think my focus personally, beyond just also the organization's focus, is thinking about like what what is privacy and surveillance mean for communities who don't have the agency to choose privacy as much as they want." (P4)

This organizer went on to posit that in addition to disproportionate power balances producing dissimilar options for individuals to protect their privacy, those with less agency are less likely to be involved in dialogues about privacy-related issues:

> "I think these privacy conversations are often reaching a very select group of people. Sometimes it's like an echo chamber of like talking about privacy and surveillance and often I think the people who are most impacted by some of these questions aren't always in the room." (P4)

Structuring privacy groups around attendees' concerns offers a chance for concerns of minoritized people to be elevated and addressed, albeit on a local level. One participant explained that often there is a one-size-fits-all approach to cybersecurity:

> "The general approach a lot of people faced when learning about cybersecurity [...] was that it was either kind of like I don't know how to explain it, but like either our way or the highway or like you do this and there's really no other sense for you to do anything else. " (P2)

Structuring to Support Critical Thinking about Privacy. In opposition to a universal, tool-centered agenda for their meetings, several organizers expressed that they preferred structuring their meetings around a topic of interest that would allow attendees to share their own connections and experiences, learn to think critically about privacy topics and strategies, and make informed decisions. This approach to structuring echoes learner-centered approaches to education and design [25, 66]:

> "We wanted to take a less top down approach to education and kind of creating try to make it more, without making it completely flat, just a little bit more horizontal. So there's a little bit less of a gap between those who are instructors and just participants, because we ultimately see that both groups have a lot to learn from each other and we don't want to yeah, we don't want to feel like we're being elitist in any way." (P2)

Another organizer explained that an important goal was to develop critical thinking about privacy and technology because new users might not be aware of all of the specific threats that they may encounter online. Rather than teaching specific technologies and tools, P3 explained that:

> "So we were on the list of computer classes, which you know it's kind of a misnomer like we're not teaching people how to use Excel or giving them practical skills necessarily but I'm teaching broader things like getting some basic theory and critical thinking when it comes to technology. We would do we have basic one of the recurring things was phishing [...] and teaching people what like bad links there on the Internet and that's not the kind of question that a new user of technology is going to think that until it's like far too late." (P3)

Another participant noted that in addition to being technically complex for beginners, encryption and communication tools were not the solution to everyone's privacy problems and advocated for what was termed "holistic security," which attempts to address the different ways that individuals experience threats to their privacy. While some attendees were concerned about the threats from governments or ISPs, others were concerned about things such as people reading email over their shoulder. Here, we see how the attendee-driven structuring helped accommodate these varied concerns under a unifying umbrella:

> "We were trying to practice or discuss this idea of holistic security. We had initially [...] tried to do like the the formal model of a CryptoParty, which is a lot of encryption tools and fairly technically complicated, but the problem is that for communication tools like PGP, if you don't know people who have already used them, they're not very useful and they're also only useful against very particular adversaries. So PGP is great if you're worried about your internet service provider or maybe the government snooping on your emails. It's not so great if you're worried about like a friend reading your emails over your shoulder or something." (P1)

P1 observes in the above quote that structuring according to attendees' concerns rendered an emphasis on technical training and solutions inadequate. Teaching people about encryption or other privacy-enhancing technologies may not have helped them address the actual threats they perceived in their lives.

4.3 Supporting: Fostering Multiple Forms of Support

While providing informational support was a primary objective of privacy group organizers we interviewed, they also discussed providing and mobilizing exchange of several other forms of support including emotional support, and affirmational support. Provision of informational and emotional support have been examined in CHI and related literature as a feature of online support groups [69], we also found evidence that affirmational support—personal validation and self-esteem—was important in privacy groups.

Provision of informational support. Getting people the information they needed was a common thread throughout our interviews. One strategy for providing strong informational support was ensuring there was accessible and approachable technical information at events. One organizer explained the consensus among their group:

> "[...] we're on the same page, there was kind of a nice emphasis on creating accessible material that doesn't shame participants for their lack of knowledge in the subject area and that's, you know, true of folks who have had you know, maybe who are less computer literate o[r] folks who are maybe more computer literate, but just don't have a lot of knowledge in this particular sector." (P2)

What P2 highlights here reflects threads that appeared throughout our interviews and were sometimes juxtaposed with other findings—for example, recall that participants noted situating events in person allowed non-technical attendees to receive direct, individualized informational support from more experienced organizers or community members. P5 explicates that although resources are available, many people are not able to invest the time required to find them, and if the informational support provided is not customized to the people they are working with then it will likely not be useful:

> "I think this gets to broader theme[s] of this sort of work. Generally, that if you're willing to invest a lot of time [...] everyone has the resources out there that people can use to address a lot these questions. The most crucial thing though is that very few people have the time to actually invest in, and so that's why it's really so important in this educational work to do the job of distilling the information into actionable formats based off of the needs of the specific groups that we are serving in that training. Because if we don't have that hyper-customized approach, you can give someone a ton of information, you can give them a stack of printouts, and it will just gather dust in the corner." (P5)

Provision of Emotional Support. For our participants, emotional support was a critical feature of privacy groups because attendees came to deal with a wide range of threats and fears. One organizer described privacy group meetings as providing a space where attendees could share their feelings about being surveilled without judgement or blame and be reminded that surveillance is a product of public policy and culture:

> "People who come to our events are the ones interested in grappling with this feeling of living in a world where they feel there's a constant invasion of privacy in one form or another, and how do I confront those feelings, both technically, but also, I think we offer just a space for people to feel that, you know, it's okay like to be surveilled in this world. It's not like an individual failure. It's one of policy and culture." (P2)

P2 further explained that if all the groups provide for people who experience harassment or stalking was a place to talk about it that was "super, we're happy with that, just a place for people to feel that they can talk about it."

Another element of the emotional support given was the establishment of a space where people were able to simply talk about their experiences, even if an ultimate "solution" that resolved the issue was not provided. An organizer described some of the experiences that brought people to privacy groups:

> "People who had experienced some form of online harassment or cyberstalking or hacking who had not been able to find help anywhere else, having maybe gone to the police, having tried to [...] deal with the problem, personally" (P1)

Returning to the concept of holistic security, one of the organizers noted the importance of physical and emotional security while acknowledging the multidimensional aspects of an individual's privacy that might not always be evident:

> "Because there's a lot that we don't know, and we approach a lot of the work we do with this idea of holistic security. So it's not just the digital that's important. It's also the physical, emotional security, which is important as well. And there could be aspects of any of that, an individual's or community's cyber, physical, or emotional security that they may not be talking about that we might not be aware of. So we don't want to give people advice that could potentially hurt them, or at the very least, not apply to them because we, you know [made] an assumption about an aspect of their [threat] model. So we, we just try it. Yeah. We try not to be assertive, we tried to be approachable." (P2)

Provision of Affirmational Support. In addition to informational and emotional support, organizers stressed the importance of providing what is referred to as affirmational support—an inclusive space for the attendees to feel validated and heard. P2 described:

> "Having the public events, allowing people to kind of put a face on who this group is, or make connections with folks and kind of network with people who are also very concerned about their cybersecurity needs, who may be in a world of people who don't see the importance of their cybersecurity concerns, that they can meet other people who be like, "Okay, well yeah, this is this other person. I feel a bit validated." (P2)

These physical spaces provide a space for validation as well as combat feelings of paranoia that might have accrued through interactions with skeptical friends or family members. P2 went on to offer that:

> "[...] just space for validation seems very important because I think a lot of times people in this field [...] are kind of written off as paranoid and um, yeah, just paranoid, like the government's listening to them that you know corporations are listening to them, which we know is true in a lot of ways, but in I think the way that even though this [is] becoming more and more popular [in] conversation. The amount of I think denial around the the data surveillance that any citizen could come into contact with knowingly or not is, it's pretty vast." (P2)

Sometimes the organizers shared personal stories about not being believed by their own friends or family members. This interviewee shared that:

> "So yeah I think that that can't be forgotten, I remember like five years ago I would talk to my family about this stuff and they'd be like you're absolutely insane that doesn't happen, I mean [the NSA] doesn't literally record every phone call and I'm like, but they do. Here's the giant data center they store [it in] in Utah. It's [a] Wikipedia page." (P3)

5 DISCUSSION

Our findings characterize how *privacy pluralism* is enacted in the real world practices of those who organize privacy groups. We looked to privacy meetup groups that serve diverse populations in order to learn from organizers the practical ways that they address the varied concerns of their audiences. We identified specific attributes about how these events were situated, were structured, and provided support that organizers valued to allow them to manage pluralistic privacy interests and concerns.

Early in this paper, we note that our goal is neither to inform a particular design, nor interrogate a particular theory. It is important to note that the nature of privacy design and privacy theory are complementary and neither supercedes the other; moreover, both are important aspects of activism. One need only look as far as Kimberlè Crenshaw's formulation of intersectionality[17] for an example of social theory that has sparked discussion and new ways of thinking and engaging with design among a generation of HCI researchers [19, 34, 54, 60]. Wong and Mulligan [74] highlight the ways that design as an activity is always entangled with a particular set of political commitments. Both design and theory are linked with social action. In this sense, although we target neither design nor conceptual contributions per se, our investigation of privacy pluralism in action can be viewed as an investigation of a form of privacy activism. Pluralism is concerned with a kind of egalitarian approach to privacy that privileges no one set of experiences over another. In our discussion, we draw inspiration from the practices of privacy groups to offer pragmatic suggestions about how pluralistic thinking about privacy can translate to action.

5.1 Situating

Organizers asserted their careful curation of a space that would support attendees with pluralistic privacy concerns. Several organizers

discussed the importance of establishing trust with the community members they were trying to reach, and why situating the meetings in public spaces was a primary strategy employed to meet this goal. One explanation was holding meetings in neutral and open spaces, as opposed to private spaces with less visibility or access, might encourage attendees from vulnerable populations to feel more comfortable approaching an unfamiliar group to discuss a sensitive topic like privacy. This finding aligns with previous work by Israni et al. with low-income members of a community-based non-profit organization that found that despite their perceived shared identity, members predominantly sought informational and emotional resources from other organizational members through offline interactions, rather than on the organization's social media platform, due to lack of interpersonal trust [29].

We also found there to be similarities between reasons that organizers valued public spaces and attributes of *hybrid spaces* in Participatory Design (PD). Previous work by Muller and Druin explores the usefulness of a hybrid space, sometimes referred to as an *in-between* or *third space*, that is shared between technology researchers and end-users in relation to PD [46]. Muller and Druin note that work in cultural theory argues that important attributes of such an in-between or third space "include challenging assumptions, learning reciprocally, and creating new ideas, which emerge through negotiation and co-creation of identities, working languages, understandings, and relationships, and polyvocal (many-voiced) discussions across and through differences" [46]. We see the potential of hybrid spaces as described by Muller and Druin to be in alignment with several of the motivations of privacy group organizers in their support of privacy pluralism. Rather than presupposing one definition of privacy, the organizers situate their events to allow space—literally—for multiple conceptions of privacy to coexist. The organizers' emphasis on establishing trust by situating the meetings in a neutral and often public space reinforces the importance of this practice not only in participatory design and research, but also in research that aims to engage diverse users.

In addition to the importance of orchestrating events in open and public spaces, privacy group organizers often spoke about situating their meetings in places that were visible and accessible to diverse audiences which sometimes included a closer physical proximity to the communities themselves. Some researchers have previously employed similar strategies. For instance, drawing inspiration from the computer clubhouses that were first opened in Boston in 1993 to work with inner city youth from educationally disadvantaged backgrounds [57], Weibert et al. [71] set up six intercultural "come_IN computer clubs" in culturally and socially diverse neighborhoods in Germany. After a ten-year study, they developed a set of guidelines on how social interactions and technological support can work in tandem in an inter-cultural and inter-generational local setting [71]. Similar to privacy group organizers, Weibert et al. advocated for an open-door policy to encourage connection to new participants and to lower formal barriers to participation. They also similarly found that the local orientation of their computer clubs fostered a strong connection to the needs and interests of their diverse constituents. We find commonalities in how privacy group organizers situate their meetings to be visible and accessible to the communities and participants they are trying to reach.

That said, situating does not always mean public and open. Our data collection was done with groups in dense urban environments with a diverse set of potential constituents. Consider for a moment an imagined privacy group in a sparsely populated rural area. Organizers of our imagined group may find other ways of situating events to ensure that participants feel safe. Would high visibility of such a group in a small community be perceived differently? Possibly. We raise the spectre of the imagined rural privacy group to highlight that situating is a context-specific endeavor, but it always aims to establish an environment that furthers the goals of the group.

5.2 Structuring

Privacy group organizers championed the importance of not structuring their meetings around pre-determined privacy solutions and pushed against addressing universal privacy concerns, emphasizing their views that privacy needs vary among individuals– a consideration aligned with Solove's advocation for a more pluralistic conception of privacy [64]. Solove built upon philosopher Ludwig Wittgenstein's argument that certain concepts are better understood as "family resemblances" that "share a network of similarities without one particular thing in common" and contends that policymakers that have had a more narrow conception of privacy have overlooked crucial privacy problems [65, p. 74].

We have seen some examples of varying judicial interpretations of privacy [14, 61]. For instance, "Jessica's Law," which was passed in California in 2006, required life-long location-based electronic monitoring of all convicted sex offenders that could be accessed by their parole officers without the parolee's knowledge [61]. This is one example in which the disclosure of information, a commonly held definition of privacy [35], is at issue. It has become common in HCI to consider local community norms when considering how to design privacy solutions [7]; however, the Jessica's Law example highlights how different stakeholders may value privacy differently. McDonald et al. [43] raised the question of power relationships within communities and who does the work of establishing community norms. Work in HCI has argued that privacy means different things to different people [31] and that privacy definitions among individuals vary [35]. But how do we as researchers address the variety of privacy conceptualizations and concerns in our work if people's concerns and needs vary in critical ways even within local communities? Strategies shared by privacy group organizers indicate that when studying privacy, even when working with specific communities or groups, such as communities of color [8] or activist communities [30], privacy group organizers do not expect individuals with the same group affiliation to have the same privacy concerns, and they structure the content of the meetings to be open to (and guided by) various concerns of the attendees.

The "topic rather than tool" approach to agenda setting that was described by a few organizers allowed space for attendees to describe their own threat models and explain what privacy meant to them. This structure is similar to privacy design approaches explored by Wong and Mulligan "that foreground social values and use design to explore and define a problem (or solution) space, including values- and critically-oriented design" [74]. They propose that certain privacy design orientations are most potent when the

conception of privacy itself is undetermined or contested and argue that design "is not just a tool for solving privacy problems, but also a tool to broaden our understanding and stretch our imagination about what privacy might entail, and encourage forward-looking, sociotechnical, and reflexive thinking about privacy." The act of proposing a topic rather than a pre-determined solution at privacy meet-ups allows for a similar exploration into the breadth and depth of people's privacy conceptions and concerns.

Returning to participatory design, work has been done in several areas of research within HCI using the framework of Community-Based Participatory Research (CBPR), which looks to community members to provide information about community needs and issues [15, 68]. CBPR researchers have prioritized working with communities they are studying to develop research questions and processes [33] and assert that developing relationships with community members can help with the co-creation of knowledge, practice, and accountability [36]. Within HCI, researchers have embraced the idea that the most pertinent definition of privacy when working with a given community is the one established by the given community [7]. This approach has been particularly important in empirical research targeting specific populations or vulnerable groups [1, 5, 32, 67]. However, it is less clear how best to proceed when different members of the group, community, or population of interest hold different privacy definitions and concerns. Learning from privacy group organizers about how they structure their meetings based on the expressed individual needs of the community members, as described in the findings above, offers some strategies or perhaps inspirations on which CBPR work could be a fruitful draw in efforts to account for privacy pluralism.

5.3 Supporting

Privacy group organizers reported that they contend with pluralistic privacy concerns by offering various types of assistance including informational, emotional, and affirmational. These qualities bear a striking similarity to those found in research on support groups [9, 16, 20, 24, 26, 28]. Guthrie and Kunkel identify support groups by their "primarily aim to provide emotional and instrumental support, to facilitate personal empowerment, to increase a sense of self-control and well-being, and to alleviate loneliness or stigmatization" [24]. In addition, "a support group is distinguished from other supportive interventions because there are no formally prescribed solutions or behavioral outcomes, the desired goals are determined by the group, participants help each other as they are helped, there are no time constraints, and participation in the group is voluntary" [24]. In addition to informational support, organizers emphasized the value of emotional support and validation. Concurrent with the rebuttal of universal privacy solutions is the acceptance of privacy issues that may not have a readily available technical solution. In these situations, we heard organizers postulate that offering emotional support and a place to be heard is the best assistance they are able to provide. We also noted that these privacy groups provide "belonging support" [26] by providing a place for individuals to co-mingle with others with shared interests and concerns and is an important function of support groups [28]. Research has suggested that the need for validation can be met when an individual is able to share emotional reactions with those who have similar experiences in support groups [13]. We contend that support groups offer a useful and powerful model for thinking about how to research and design in the context of privacy pluralism.

We also propose that the value organizers placed on providing multiple types of support could be useful in thinking about designing for privacy. For instance, tools such as non-tracking browsers (e.g., incognito mode or private browsing) often provide users the ability to limit the amount of tracking performed by their internet browser. However, they have limited abilities to prevent third parties from tracking the user [3]. Although some individuals may not fully understand what these private browsers do and what they cannot do [22, 75], the technical benefits might not be the priority. Rather, the emotional component, the need to feel as if you are taking some modicum of control over your online data, may take precedence and drive the use of such tools. Thus, in addition to determining how best to address misconceptions, privacy research would likely benefit from examining the role that emotional motivations—feelings of well-being, validation, and agency—play in the use of privacy technologies and practices.

6 LIMITATIONS AND FUTURE WORK

Our sample focuses on the perspectives of privacy group organizers who plan events in large urban areas in the United States. Future work could investigate the experiences of privacy group participants, as well as privacy groups that operate beyond the limited geographical scope and context of our study, for example in rural areas. Future work should also engage not only with organizers but also with attendees and participants to examine how the various practices described here (situating meetings, structuring meetings, and providing support) are perceived and experienced by those they are intended to serve. Finally, interview-based research seeks to access participants' experiences and how they make meaning of those experiences; as such, it is necessarily bounded by the specific group of people interviewed. Although participant selection introduces limitations to any given interview-based study, it must be acknowledged as a characteristic of the research method.

7 CONCLUSION

We performed ethnographic fieldwork and an interview study with six individuals involved with the organization of privacy meetup groups in diverse urban communities to see how they contend with privacy pluralism in practice. We identified three dimensions of organizing privacy groups that serve diverse audiences: situating, structuring, and providing support. Situating the event included finding the right physical or virtual space, structuring meetings involved creating an open format guided by participants, and providing support included informational and emotional support. We used these findings as a guide in a discussion of "privacy pluralism" and proposed how they might inform practices within the HCI privacy research community.

ACKNOWLEDGMENTS

This work was supported by the National Science Foundation (Awards #1816264 and #1814533). The findings and recommendations in this paper are those of the authors and do not necessarily

reflect the views of the NSF. Thanks to the participants and the organizers' groups for their willingness to be involved in our work.

REFERENCES

[1] Norah Abokhodair and Sarah Vieweg. 2016. Privacy & social media in the context of the Arab Gulf. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*. ACM, Brisbane QLD Australia, 672–683. https://doi.org/10.1145/2901790.2901873

[2] Tanisha Afnan, Yixin Zou, Maryam Mustafa, Mustafa Naseem, and Florian Schaub. 2022. Aunties, strangers, and the FBI: Online privacy concerns and experiences of Muslim-American women. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 387–406.

[3] Gaurav Aggarwal, Elie Bursztein, Collin Jackson, and Dan Boneh. 2010. An analysis of private browsing modes in modern browsers. In *19th USENIX Security Symposium (USENIX Security 10)*. USENIX Association, Washington, D.C.

[4] Syed Ishtiaque Ahmed, Md. Romael Haque, Jay Chen, and Nicola Dell. 2017. Digital privacy challenges with shared mobile phone use in Bangladesh. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (Dec. 2017), 1–20. https://doi.org/10.1145/3134652

[5] Syed Ishtiaque Ahmed, Md Romael Haque, Shion Guha, Md Rashidujjaman Rifat, and Nicola Dell. 2017. Privacy, security, and surveillance in the Global South: A study of biometric mobile SIM registration in Bangladesh. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 906–918. https://doi.org/10.1145/3025453.3025961

[6] UN General Assembly et al. 1948. Universal declaration of human rights. *UN General Assembly* 302, 2 (1948), 14–25.

[7] Louise Barkhuus. 2012. The mismeasurement of privacy: Using contextual integrity to reconsider privacy in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Austin, Texas, USA) *(CHI '12)*. Association for Computing Machinery, New York, NY, USA, 367–376. https://doi.org/10.1145/2207676.2207727

[8] Alvaro M Bedoya. 2020. Privacy as civil right. *New Mexico Law Review* 50 (2020), 301.

[9] Jacqueline L. Bender, Maria-Carolina Jimenez-Marroquin, and Alejandro R. Jadad. 2011. Seeking support on Facebook: A content analysis of breast cancer groups. *Journal of Medical Internet Research* 13, 1 (2011), e16. https://doi.org/10.2196/jmir.1560

[10] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (Jan. 2006), 77–101. https://doi.org/10.1191/1478088706qp063oa

[11] Moritz Büchi. 2021. Digital inequalities in online privacy protection: Effects of age, education and gender. In *Handbook of Digital Inequality*. Edward Elgar Publishing, 296–310. https://doi.org/10.4337/9781788116572.00029

[12] Hichang Cho, Bart Knijnenburg, Alfred Kobsa, and Yao Li. 2018. Collective privacy management in social media: A cross-cultural validation. *ACM Transactions on Computer-Human Interaction* 25, 3 (June 2018), 1–33. https://doi.org/10.1145/3193120

[13] Dan Coates and Tina Winston. 1983. Counteracting the deviance of depression: Peer support groups for victims. *Journal of Social Issues* 39, 2 (July 1983), 169–194. https://doi.org/10.1111/j.1540-4560.1983.tb00147.x

[14] Thomas D Colbridge. 2001. Kyllo v. United States: Technology versus individual privacy. *FBI L. Enforcement Bull.* 70 (2001), 25. HeinOnline.

[15] Ned Cooper, Tiffanie Horne, Gillian R Hayes, Courtney Heldreth, Michal Lahav, Jess Holbrook, and Lauren Wilcox. 2022. A systematic review and thematic analysis of community-Collaborative approaches to computing research. In *CHI Conference on Human Factors in Computing Systems*. ACM, New Orleans LA USA, 1–18. https://doi.org/10.1145/3491102.3517716

[16] Neil S. Coulson, Heather Buchanan, and Aimee Aubeeluck. 2007. Social support in cyberspace: A content analysis of communication within a Huntington's Disease online support group. *Patient Education and Counseling* 68, 2 (Oct. 2007), 173–178. https://doi.org/10.1016/j.pec.2007.06.002

[17] Kimberle Crenshaw. 1990. Mapping the margins: Intersectionality, identity politics, and violence against women of color. *Stanford Law Review* 43 (1990), 1241.

[18] Dmitry Epstein and Kelly Quinn. 2020. Markers of online privacy marginalization: Empirical examination of socioeconomic disparities in social media privacy attitudes, literacy, and behavior. *Social Media + Society* 6, 2 (April 2020), 205630512091685. https://doi.org/10.1177/2056305120916853

[19] Sheena Erete, Yolanda A Rankin, and Jakita O Thomas. 2022. A method to the madness: Applying an intersectional analysis of structural oppression and power in HCI and design. *ACM Transactions on Computer-Human Interaction* (2022). https://doi.org/10.1145/3507695

[20] Marilyn Evans, Lorie Donelle, and Laurie Hume-Loveland. 2012. Social support and online postpartum depression discussion groups: A content analysis. *Patient Education and Counseling* 87, 3 (June 2012), 405–410. https://doi.org/10.1016/j.pec.2011.09.011

[21] Luciano Floridi. 2005. The ontological interpretation of informational privacy. *Ethics and Information Technology* 7, 4 (Dec. 2005), 185–200. https://doi.org/10.1007/s10676-006-0001-7

[22] Xianyi Gao, Yulong Yang, Huiqing Fu, Janne Lindqvist, and Yang Wang. 2014. Private browsing: An inquiry on usability and privacy protection. In *Proceedings of the Workshop on Privacy in the Electronic Society (WPES)*. ACM, Scottsdale, AZ, 97–106. https://doi.org/10.1145/2665943.2665953

[23] Seda Gurses and Jose M. del Alamo. 2016. Privacy engineering: Shaping an emerging field of research and practice. *IEEE Security & Privacy* 14, 2 (March 2016), 40–46. https://doi.org/10.1109/MSP.2016.37

[24] Jennifer A. Guthrie and Adrianne Kunkel. 2015. Communication in support groups. In *The International Encyclopedia of Interpersonal Communication* (1 ed.), Charles R Berger, Michael E Roloff, Steve R Wilson, James Price Dillard, John Caughlin, and Denise Solomon (Eds.). Wiley, 1–5. https://doi.org/10.1002/9781118540190.wbeic034

[25] Idit Harel and Seymour Papert (Eds.). 1991. *Constructionism.* Ablex Publishing.

[26] Julianne Holt-Lunstad and Briahna Bushman. 2015. Social relationships and physical health: Are we better or worse off because of our relationships? *Relationships and Psychology: A Practical Guide* (2015), 399.

[27] Hsiao-Ying Huang and Masooda Bashir. 2018. Surfing safely: Examining older adults' online privacy protection behaviors. *Proceedings of the Association for Information Science and Technology* 55, 1 (Jan. 2018), 188–197. https://doi.org/10.1002/pra2.2018.14505501021

[28] Jodie Huff. 2015. Parent to parent, peer to peer: An investigation of mutual social support groups as a resource for genetic counselors. [Dissertation]. (2015). Brandeis University, Graduate School of Arts and Sciences.

[29] Aarti Israni, Nicole B Ellison, and Tawanna R Dillahunt. 2021. "A library of people": Online resource-seeking in low-income communities. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (2021), 1–28. https://doi.org/10.1145/3449226 ACM New York, NY, USA.

[30] Haiyan Jia and Eric P. S. Baumer. 2022. Birds of a feather: Collective privacy of online social activist groups. *Computers & Security* 115 (April 2022), 102614. https://doi.org/10.1016/j.cose.2022.102614

[31] John Karat, Clare-Marie Karat, and Carolyn Brodie. 2007. Human-computer interaction viewed from the intersection of privacy, security, and trust. In *The Human-Computer Interaction Handbook*. CRC Press, 665–684.

[32] Naveena Karusala, Apoorva Bhalla, and Neha Kumar. 2019. Privacy, patriarchy, and participation on social media. In *Proceedings of the ACM Conference on Designing Interactive Systems (DIS)*. ACM, San Diego, CA, 511–526. https://doi.org/10.1145/3322276.3322355

[33] Rhonda Koster, Kirstine Baccar, and R. Harvey Lemelin. 2012. Moving from research ON, to research WITH and FOR Indigenous communities: A critical reflection on community-based participatory research. *The Canadian Geographer / Le Géographe canadien* 56, 2 (June 2012), 195–210. https://doi.org/10.1111/j.1541-0064.2012.00428.x

[34] Neha Kumar and Naveena Karusala. 2019. Intersectional computing. *Interactions* 26, 2 (2019), 50–54.

[35] Michelle Kwasny, Kelly Caine, Wendy A. Rogers, and Arthur D. Fisk. 2008. Privacy and technology: Folk definitions and perspectives. In *CHI '08 Extended Abstracts on Human Factors in Computing Systems*. ACM, Florence Italy, 3291–3296. https://doi.org/10.1145/1358628.1358846

[36] Sarah de Leeuw, Emilie S. Cameron, and Margo L. Greenwood. 2012. Participatory and community-based research, Indigenous geographies, and the spaces of friendship: A critical engagement. *The Canadian Geographer / Le Géographe canadien* 56, 2 (June 2012), 180–194. https://doi.org/10.1111/j.1541-0064.2012.00434.x

[37] Amanda Lenhart, Mary Madden, Sandra Cortesi, Urs Gasser, and Aaron Smith. 2013. Where teens seek online privacy advice. *Pew Research Center, Internet & Technology* (2013). https://www.pewresearch.org/internet/2013/08/15/where-teens-seek-online-privacy-advice/

[38] Tianshi Li, Elizabeth Louie, Laura Dabbish, and Jason I. Hong. 2021. How developers talk about personal data and what it means for user privacy: A case study of a developer forum on Reddit. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (Jan. 2021), 1–28. https://doi.org/10.1145/3432919

[39] Sun Sun Lim, Hichang Cho, and Milagros Rivera Sanchez. 2009. Online privacy, government surveillance and national ID cards. *Commun. ACM* 52, 12 (Dec. 2009), 116–120. https://doi.org/10.1145/1610252.1610283

[40] Yvonna S Lincoln and Egon G Guba. 1985. *Naturalistic inquiry.* Sage.

[41] Jacob Logas, Ari Schlesinger, Zhouyu Li, and Sauvik Das. 2022. Image DePO: Towards gradual decentralization of online social networks using decentralized privacy overlays. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW1 (March 2022), 1–28. https://doi.org/10.1145/3512907

[42] Mary Madden. 2017. Privacy, security, and digital inequality. (2017).

[43] 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*. 1–8. https://doi.org/10.1145/3334480.3375174

[44] 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

[45] Vikram Mehta, Daniel Gooch, Arosha Bandara, Blaine Price, and Bashar Nuseibeh. 2021. Privacy care: A tangible interaction framework for privacy management. *ACM Transactions on Internet Technology* 21, 1 (Feb. 2021), 1–32. https://doi.org/10.1145/3430506

[46] Michael J Muller and Allison Druin. 2012. Participatory design: The third space in human–computer interaction. In *The human–computer interaction handbook*. CRC Press, 1125–1153.

[47] Deirdre K. Mulligan, Colin Koopman, and Nick Doty. 2016. Privacy is an essentially contested concept: A multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374, 2083 (Dec. 2016), 20160118. https://doi.org/10.1098/rsta.2016.0118

[48] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Washington Law Review* 79 (2004), 119.

[49] Helen Nissenbaum. 2010. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, Stanford, CA.

[50] Helen Nissenbaum. 2011. A contextual approach to privacy online. *Daedalus* 140, 4 (Sept. 2011), 32–48. https://doi.org/10.1162/DAED_a_00113

[51] Leysia Palen and Paul Dourish. 2003. Unpacking "privacy" for a networked world. In *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI)*. Ft. Lauderdale, FL, 129–136. https://doi.org/10.1145/642633.642635

[52] Sandra Petronio. 1991. Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication Theory* 1, 4 (Nov. 1991), 311–335. https://doi.org/10.1111/j.1468-2885.1991.tb00023.x

[53] Sandra Petronio. 2002. *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press, Albany, NY.

[54] Yolanda A Rankin, Jakita O Thomas, and Nicole M Joseph. 2020. Intersectionality in HCI: Lost in translation. *Interactions* 27, 5 (2020), 68–71.

[55] Elissa M Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L Mazurek. 2020. A comprehensive quality evaluation of security and privacy advice on the web. In *29th USENIX Security Symposium (USENIX Security 20)*. 89–108.

[56] Matt Reichel. 2017. Race, class, and privacy: A critical historical review. *International Journal of Communication* 11 (2017), 4757–4768.

[57] Mitchel Resnick and Natalie Rusk. 1996. The computer clubhouse: Preparing for life in a digital world. *IBM Systems Journal* 35, 3.4 (1996), 431–439. IBM.

[58] Mohammad Rashidujjaman Rifat, Mahiratul Jannat, Mahdi Nasrullah Al-Ameen, S M Taiabul Haque, Muhammad Ashad Kabir, and Syed Ishtiaque Ahmed. 2021. Purdah, amanah, and gheebat: Understanding privacy in Bangladeshi "pious" Muslim communities. In *ACM SIGCAS Conference on Computing and Sustainable Societies (COMPASS)*. ACM, Virtual Event Australia, 199–214. https://doi.org/10.1145/3460112.3471957

[59] Shruti Sannon and Andrea Forte. 2022. Privacy research with marginalized groups: What we know, what's needed, and what's next. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 1–33.

[60] 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*. 5412–5427.

[61] Irina Shklovski, Janet Vertesi, Emily Troshynski, and Paul Dourish. 2009. The commodification of location: Dynamics of power in location-based systems. In *Proceedings of the International Conference on Ubiquitous Computing (Ubicomp)*. Orlando, FL, 11–20. https://doi.org/10.1145/1620545.1620548

[62] Cristiana S. Silva, Glívia A.R. Barbosa, Ismael S. Silva, Tatiane S. Silva, Fernando Mourão, and Flávio Coutinho. 2017. Privacy for children and teenagers on social networks from a usability perspective: A case study on Facebook. In *Proceedings of the 2017 ACM on Web Science Conference*. ACM, Troy New York USA, 63–71. https://doi.org/10.1145/3091478.3091479

[63] Patrick Skeba and Eric P. S. Baumer. 2020. Informational friction as a lens for studying algorithmic aspects of privacy. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (Oct. 2020), 101:1–101:22. https://doi.org/10.1145/3415172

[64] Daniel J Solove. 2008. Understanding privacy. (2008). Harvard University Press.

[65] Daniel J. Solove. 2015. The meaning and value of privacy. In *Social Dimensions of Privacy* (1 ed.), Beate Roessler and Dorota Mokrosinska (Eds.). Cambridge University Press, 71–82. https://doi.org/10.1017/CBO9781107280557.005

[66] Elliot Soloway, Mark Guzdial, and Kenneth E Hay. 1994. Learner-centered design: The challenge for HCI in the 21st century. *interactions* 1, 2 (1994), 36–48.

[67] Sara Vannini, Ricardo Gomez, and Bryce Clayton Newell. 2020. "Mind the five": Guidelines for data privacy and security in humanitarian work with undocumented migrants and other vulnerable populations. *Journal of the Association for Information Science and Technology* 71, 8 (Aug. 2020), 927–938. https://doi.org/10.1002/asi.24317

[68] Nina B. Wallerstein and Bonnie Duran. 2006. Using community-based participatory research to address health disparities. *Health Promotion Practice* 7, 3 (July 2006), 312–323. https://doi.org/10.1177/1524839906289376

[69] Yi-Chia Wang, Robert Kraut, and John M. Levine. 2012. To stay or leave?: The relationship of emotional and informational support to commitment in online health support groups. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work - CSCW '12*. ACM Press, Seattle, Washington, USA, 833. https://doi.org/10.1145/2145204.2145329

[70] Samuel D. Warren and Louis D. Brandeis. 1890. The right to privacy. *Harvard Law Review* 4, 5 (1890), 193–220. https://doi.org/10.2307/1321160

[71] Anne Weibert, Mary-Ann Sprenger, Dave Randall, and Volker Wulf. 2016. Lifecycles of computer clubs: Rhythms and patterns of collaboration and learning in an intercultural setting. In *Proceedings of the 19th International Conference on Supporting Group Work*. ACM, Sanibel Island Florida USA, 137–147. https://doi.org/10.1145/2957276.2957306

[72] Wikipedia. 2022. CryptoParty. (1 April 2022). https://en.wikipedia.org/w/index.php?title=CryptoParty&oldid=1081462848

[73] Rhiannon Williams. 2020. Google says everyone's online privacy red lines are different and change over time. *Technology* (Feb. 2020). https://inews.co.uk/news/technology/google-online-privacy-different-things-different-people-gdpr-privacy-399890

[74] Richmond Y Wong and Deirdre K Mulligan. 2019. Bringing design to the privacy table: Broadening "Design" in "Privacy by Design" through the lens of HCI. 1–17.

[75] Yuxi Wu, Panya Gupta, Miranda Wei, Yasemin Acar, Sascha Fahl, and Blase Ur. 2018. Your secrets are safe: How browsers' explanations impact misconceptions about private browsing mode. In *Proceedings of the 2018 World Wide Web Conference (WWW '18)*. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 217–226. https://doi.org/10.1145/3178876.3186088

[76] Shoshana Zuboff. 2015. Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology* 30, 1 (March 2015), 75–89. https://doi.org/10.1057/jit.2015.5