# Reflexivity & Reflection (R&R) for Sociotechnical Safety: Creating a Space for Collective Learning


Jessica McClearn*
Information Security Group
Royal Holloway University of London
London, United Kingdom
jessica.mcclearn.2021@live.rhul.ac.uk

Lucy Qin*
Georgetown University
Washington D.C., USA
lucy.qin@georgetown.edu

Emily Tseng*
Microsoft Research
New York, USA
University of Washington
Seattle, USA
etseng42@gmail.com

Miranda Wei*
Princeton University
Princeton, USA
mirandaaa.wei@gmail.com

Rikke Bjerg Jensen†
Information Security Group
Royal Holloway University of London
London, United Kingdom
rikke.jensen@rhul.ac.uk

Nora McDonald†
George Mason University
Fairfax, USA
nmcdona4@gmu.edu

Elissa M. Redmiles†
Computer Science
Georgetown University
Washington D.C., USA
elissa.redmiles@georgetown.edu

Morgan Klaus Scheuerman†
Sony AI
Boulder, USA
morgan.scheuerman@sony.com

Reem Talhouk†
School of Design
Northumbria University
Newcastle-upon-Tyne, United Kingdom
reem.talhouk@northumbria.ac.uk



## Abstract

Researchers in CSCW have long examined the sociotechnical aspects of digital security, privacy, and safety, building knowledge not only on the security challenges faced by (at-risk) communities, but also on the challenges of conducting responsible research. The burgeoning subfield of "sociotechnical safety" within computer security & privacy (S&P) has grown alongside this work, including topics like the S&P of at-risk users. These two research fields are distinct in epistemological and methodological approaches, but share a common goal: improving the digital safety of (at-risk) populations. During this critical time, we see an opportunity to gather as one community, to encourage honest conversation about the "hows" and "whys" of sociotechnical safety research. We invite researchers in both fields to discuss how CSCW's methods, norms, and theories might bridge this emergent community, e.g., building meaningful collaborations with participants, researcher/participant safety. To cultivate reflexivity and reflection (R&R), we will host a closed-door panel of experienced researchers to share learnings from their work before collaboratively developing artifacts outlining actions that researchers can take to address these challenges. By fostering a collective learning environment at CSCW, we will assist researchers across disciplines to conduct responsible sociotechnical safety research by prioritising reflexivity.



## CCS Concepts

• **Security and privacy** → **Social aspects of security and privacy**; • **Human-centered computing** → **Computer supported cooperative work**; **User studies**.

## Keywords

Reflexivity, reflection, sociotechnical safety, collective learning, digital safety.

**ACM Reference Format:**
Jessica McClearn, Lucy Qin, Emily Tseng, Miranda Wei, Rikke Bjerg Jensen, Nora McDonald, Elissa M. Redmiles, Morgan Klaus Scheuerman, and Reem Talhouk. 2025. Reflexivity & Reflection (R&R) for Sociotechnical Safety: Creating a Space for Collective Learning. In *Companion of the Computer-Supported Cooperative Work and Social Computing (CSCW Companion '25), October 18–22, 2025, Bergen, Norway*. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3715070.3748292


## 1 Motivation

CSCW scholarship has increasingly included research on topics of safety, security, and privacy in a range of contexts, such as on social media [1, 16, 28], in online communities [8, 31], and in the harms caused by AI [32, 33], among many others. CSCW scholars have reflected on the practices and approaches within their work, such as how studies of privacy and power for at-risk populations are framed [26, 27] or how to collaborate with communities to investigate safety needs [22, 35, 37]. Through these contributions, CSCW has established new methods, norms, and theories for how to do

*All co-organizers contributed equally.
†All panelists contributed equally.



*CSCW Companion '25, Bergen, Norway*



ACM ISBN 979-8-4007-1480-1/25/10
https://doi.org/10.1145/3715070.3748292

research on security and privacy at the social and technical intersection, and what "sociotechnical safety" encompasses [38]. In parallel, computer security and privacy (S&P) researchers increasingly scope their research to include populations who face heightened security and privacy threats [18, 25, 39]. Such populations, referred to as "at-risk users" in the S&P community, are now explicitly included in top S&P venues' Call for Papers.[1] S&P researchers are grappling with how to do this research ethically [3, 19] and safely [2], and how to create new spaces to discuss the social factors relevant to S&P.[2]

In both the CSCW and S&P communities, researchers share a common goal: improving safety for people suffering in ways accelerated by our sociotechnical world. Yet, to-date, there have been scant opportunities for the two growing subfields to connect over *how* to do such research: S&P scholars often miss CSCW's theoretical frameworks and critical reflection in their accounts of security behaviors, and CSCW scholars miss S&P's knowledge of operational security in their efforts to design securely. To achieve our common goal of improving safety for all, we need to look at *how* we do this research by bridging conversations about the methods, norms, and theories across these two communities. Our Reflexivity & Reflection (R&R) session, will create that bridge by gathering sociotechnical safety researchers across CSCW and S&P as one community. We will create a closed space for honest conversations about the "hows" and "whys" of sociotechnical safety research, and facilitate collective learning among researchers at all levels. We will do this by embedding in this growing community CSCW's scholarship on researcher *reflexivity*.

Reflexivity starts with acknowledging that knowledge is the product of the researcher's subjective lens: "*a living, contradictory, vulnerable, evolving multiple self, who speaks in a partial, subjective, culture-bound voice*" [13]. From that understanding, researchers must learn to embed self-reflection into their practices. Further, collective reflection enables opportunities for researchers to learn from each others' experiences, but requires careful scaffolding. Researchers themselves, must feel safe enough to be vulnerable with each other and constructively criticize each other's experiences. We therefore adopt a new panel format by drawing from fields beyond computing, where spaces for collective reflection have been developed; morbidity and mortality (M&M) conferences where (typically senior) medical doctors to speak candidly about issues raised by adverse patient outcomes [15, 30]. Inspired by M&Ms and their culture of collective learning we are excited to bring this novel approach to HCI and S&P researchers at CSCW, and convene a space for Reflexivity and Reflection (R&R) in sociotechnical safety. As this space will be hosted in Norway, we are also inspired by Scandanavian foundations and approaches to participatory design in our exploration of reflexivity that emphasizes interactions, inclusivity and collaboration between researchers, participants and sites of research [4, 12, 20, 34]. We will explore the following themes:

(1) **How can safety researchers navigate their own positionality?** When research requires deeply understanding another person's felt sense of (un)safety, how can researchers understand the impact of their own presence on participants' lives? We will explore the relationship between our own positionalities as researchers and the communities we work with, including how to navigate responsibilities to our topics, field sites, colleagues, careers, participants, and community partners.
(2) **What does responsible research look like for the field of sociotechnical safety?** Particular attention will be given in relation to working with populations from diverse contexts and with diverse safety needs, looking to existing CSCW work in this field [24] and more broadly across security and privacy research [3].
(3) **How do you select or develop appropriate methods?** CSCW has provided a home for diverse methodologies to converge, providing fertile ground for a discussion on navigating methodological choices in relation to safety research contexts and goals. We will reflect on advantages and disadvantages of methods common or emerging in sociotechnical safety research [2, 24, 40].
(4) **What best practices can we establish for researcher safety in this field?** Researchers working in this area may incur personal harm, such as long-term mental health effects from working with emotionally distressing or traumatic research data [10, 21, 29], or harassment from individuals who seek to harm researchers [6, 7]. We hope to develop dialogue on researcher well-being and build upon prior work to create shared resources [11, 29].

We propose this workshop at a time where sociotechnical safety, especially of at-risk populations, is an urgent priority. The past 12-months has witnessed changing geopolitical conditions, that has impacted research priorities and funding sources. We have a responsibility to foster reflexivity to ensure ethical and sustainable sociotechnical safety research can continue. Our panel format, where senior researchers are invited to speak candidly in a closed session (similar to the Chatham House Rule[3]), experiments with discreet methods to support researchers in navigating challenges to safety research given the current political climate.

## 2 Organizing Team

The organizing team includes an experienced and diverse group of researchers and students who are intimately aware of the intersection of identity and safety. The team represents seven different institutions (across academia and industry) who use different research approaches (trauma-informed, feminist, decolonial, participatory design, everyday and collective security) and methodologies (ethnographic, qualitative, computational, cryptographic, economic and mixed methods) across CSCW and S&P. Collectively, we have published work at CSCW and other top-tier venues in social computing (ACM CHI), as well as at top-tier venues in S&P (USENIX Security, IEEE S&P).

**Jessica McClearn** is a PhD candidate at Royal Holloway University of London in the Center for Doctoral Training in Cyber

[1] https://www.usenix.org/conference/usenixsecurity24/call-for-papers
[2] For example, Re-Imagining Cryptography and Privacy (ReCAP) workshop (https://recapworkshop.online/), Gender, Online Safety, and Sexuality (GOSS) workshop (https://gossworkshop.github.io/), the Workshop on Inclusive Privacy and Security (WIPS) (https://inclusiveprivacy.org/workshops/wips2023.html), and the Social Foundations of Cryptography project (https://social-foundations-of-cryptography.gitlab.io/about).
[3] https://www.chathamhouse.org/about-us/chatham-house-rule

Security for the Everyday. She utilizes ethnographically informed methods to consider digital and ontological security practices of populations impacted by conflict.

**Lucy Qin** is a postdoctoral fellow at Georgetown University within the Initiative for Tech & Society. Lucy completed her PhD in computer science at Brown University in 2023, where the focus of her work was on developing usable privacy tools.

**Emily Tseng** is a postdoctoral researcher at Microsoft Research, and will join the faculty of the University of Washington in spring 2026. She is broadly interested in how technology mediates harm, how to intervene, and what it means to do so. Emily's PhD at Cornell Information Science examined digital technologies' role in intimate partner violence. She has organized successful hybrid workshops at ACM CSCW [22, 23, 41], CHI [9], and FAccT.

**Miranda Wei** is a postdoctoral researcher at Princeton University. Their work investigates how gender, interpersonal relationships, and other social discourses shape people's security, privacy, and online safety. They is particularly interested investigating how sociotechnical harms arise from emerging technologies and on social media. In 2024, they organized a successful hybrid workshop at SOUPS. [4]

**Rikke Bjerg Jensen** is a social scientist and a reader (≈associate professor) in the Information Security Group at Royal Holloway University of London. Her work is distinctly ethnographic in nature and explores information security needs, perspectives and practices among groups often living and working at what we might call the margins of societies.

**Nora McDonald** is an assistant professor at George Mason University in Information Sciences and Technology. She studies the privacy practices of vulnerable populations and the impact of complex surveillance ecosystems and data relations on our shifting norms around privacy. She is interested in how people threat model in the context of reproductive health.

**Morgan Klaus Scheuerman** is a research scientist on Sony AI's AI Ethics team and a visiting scholar in Information Science at University of Colorado Boulder. Morgan broadly focuses on mitigating technical harms, particularly in the context of AI development and deployment. Much of his work has examined how computer vision systems construct identity, and how that construction disempowers marginalized groups.

**Elissa M. Redmiles** is the Clare Luce Boothe Assistant Professor of Computer Science at Georgetown University and a Faculty Associate at the Berkman Klein Center for Internet & Society at Harvard University. She uses computational, economic, and social science methods to understand users' security, privacy, and online safety-related decision-making processes, with a particular focus on safety in intimate interactions.

**Reem Talhouk** is an Assistant Professor in Design and Global Development at Northumbria University, where she also co-leads the 'Design Feminisims' and 'MARGINALITIES' research groups. She has conducted research with refugees, activists and humanitarians, with a focus on the interplay between sociotechnical systems and mechanisms of oppression and resistance.

[4] https://gossworkshop.github.io/

# 3 Planned Activities

## 3.1 Pre-Workshop: Pilot Panel, Asynchronous Connections and Online Preparation

*Pilot Panel.* In August 2025, prior to our workshop, we will test the reflexivity and reflection (R&R) model by piloting our panel within a workshop at SOUPS, a conference about human-computer interaction and computer security and privacy (S&P). The Gender, Online Safety, and Sexuality (GOSS) workshop at SOUPS will convene in 2025 for its second iteration; the goal of GOSS is to gather community around the study of online safety through the lenses of gender and sexuality. In this iteration of GOSS, our pilot panel on R&R will foster deeper reflection on the *hows* of sociotechnical S&P research. By hosting this panel at SOUPS it further actions our commitment to bridge S&P and CSCW by encouraging multiple points of engagement for panelists and participants and transferring lessons learned. We will promote this CSCW workshop to the SOUPS workshop attendees to encourage joint participation.

*Asynchronous connections before CSCW commences.* We will host asynchronous activities to help participants (a) become familiar with each others' work; (b) ground their thinking in the workshop's themes; and (c) establish working agreements. Following [22], each participant will introduce themselves, their work, and their goals in a single slide on a **biographical slide deck** shared in a Slack channel. This deck will facilitate mutual introductions, and organizers will prompt participants to connect with one individual they had not previously met in advance of the workshop.

Second, we will organize a **shared annotated bibliography on sociotechnical safety across CSCW and S&P**. The organizers will seed the bibliography to concretely demonstrate topics in our definition of sociotechnical safety and encourage participants to contribute texts and/or annotations to this living document. The purpose of this annotated bibliography is both to ground participants in ideas relevant to the workshop themes and to create the foundations for a future resource on sociotechnical safety. Finally, we will circulate **working agreements** to establish guidelines for engaging in what can be a vulnerable space for reflection. We aim to center respect, collaboration, individual and collective learning, and celebrating differences during our workshop. We will ask participants to review, reflect, and make edits to the working agreements (see initial list in Appendix A).

## 3.2 Live Hybrid Workshop: R&R Panel and Artifact Development

Following a Freirean pedagogical model of cycles of reflection and action [14] (aligning with prior CSCW workshops [22, 36]), we will begin in a facilitated *reflection* centered on an expert panel in an M&M style which we have penned R&R. After a meal break, we will *commit to action* in small groups by working on artifacts addressing the challenges raised.

*3.2.1 Activity 1: Reflection via Expert Panel.* We will begin with an R&R in the style of an expert panel, moderated by members of the organizing team. Each of our expert panelists (Scheuerman, McDonald, Redmiles, Talhouk, Jensen) will take 5-6 minutes to (a)

introduce themselves and their work and (b) reflect on a methodological, ethical, or structural challenge they have faced in their sociotechnical safety research. The moderators will ask questions and encourage crosstalk between expert panelists, to model supportive, critical reflection. We will follow this panel with an audience Q&A.

At the conclusion of the panel, we will invite participants to reflect on content from the panel and share a learning they will take forward in their own research practices which will be shared through a digital interactive board (e.g., Miro, Jamboard). This will be revisited to identify topics for the following activity.

*3.2.2 Activity 2: Action via Artifact Development.* Following our expert panel, we will turn towards *action* and how these challenges can be addressed through our collective effort as a community. The organizers will organize questions accumulated during the morning's reflections and pre-workshop activities to develop a list of *community challenges*—common barriers, both structural and practical, that affect scholars in sociotechnical safety across disciplines.

Participants will take 20-30 minutes to pick a challenge that they would like to work on in groups. Participants will spend the afternoon working on *artifacts* to address their selected challenges. These artifacts could include formal academic outputs (e.g., reviews, research proposals, papers) or community resources (e.g., shared syllabi, best practices, shared datasets) or creative outputs (e.g., a collage, spoken-word piece, zine).

Workshop organizers will rotate between small groups to support the work and connect participants to resources where needed. The workshop will conclude with a share-out in which each group describes their challenge, their artifact, possibilities to continue their work, and opportunities for others to get involved.

*3.2.3 Proposed Schedule.* Our schedule is modularized and easily adjusted to accommodate CSCW's coffee breaks.
9:30am-10:00am: Welcome
10:00am-10:30am: Participant Introductions
10:30am-12:00pm: Activity 1: Researcher Panel and Q&A
12:00pm-1:30pm: Lunch. Optional small groups organized by themes.
1:30pm-3:00pm: Activity 2: Artifact Development.
3:00pm-3:30pm: Break
3:30pm-5:00pm: Share-out and wrap-up.

*3.2.4 Modality.* This will be a **one-day, hybrid** workshop at CSCW 2025. A hybrid modality will further our goal of collective learning, enabling accessibility and inclusivity. The organizers are experienced at running dual online and in-person workshops, including 4+ hybrid workshops across the team, and bring expertise on creating an integrated hybrid space. We will encourage in-person participants to have their laptops available to continue a continuous connection with online participants.

*3.2.5 Equipment and Supplies.* The majority of our workshop will be conducted via virtual spaces (e.g., Google docs, Zoom and Slack) to facilitate an active hybrid environment. We require internet connectivity at the venue, and request a projector, screen, and camera if available. We will need tables and seating for in-person panelists and participants. We will lastly require three microphones (one for panelists, one for a moderator, and one for audience questions).

# 4 Participation: Recruitment and Accessibility

## 4.1 Recruitment

We welcome participants from diverse backgrounds with different identities, geographies, disciplines and levels of experience with sociotechnical safety research. We will actively encourage Global Majority participation by sharing the CFP broadly through our international connections as well as publicly accessible mailing lists, on social media, and similar channels. Finally, we also aim to build community between junior and senior researchers, so that collective learning will not be restricted to one cohort of researchers.

The CFP will ask for a short (maximum 500 words) reflection including (a) an introduction to prospective participants' prior, current, and aspirational work in sociotechnical safety; and (b) a methodological, ethical, or structural challenge they face as researchers that they would like to discuss in this space. In order to facilitate our goals of honest and transparent discussion, we will cap participation at **25 people, including workshop organizers**.

## 4.2 Accessibility

We intend to create a space that allows for full participation by all attendees. When registering, participants will be asked for any accommodations in order to access the workshop of which we will make our best effort to fulfill and accommodate. At minimum, we will turn on auto-captioning for virtual participants on Zoom and we will ensure that microphones are used by panelists and those asking questions.

# 5 Expected Outcomes

This workshop will bring together researchers across CSCW, S&P, and social computing towards:

(1) **Establishing a joint community between CSCW and S&P researchers.** Given the range of the workshop participants' knowledge and expertise, we aim to cultivate alliances between CSCW, HCI, and computer S&P researchers to grow a community around sociotechnical safety. We will continue these connections through the Slack channel and host variations of this R&R in different HCI and S&P venues to continue fostering these conversations and bring forward learnings from CSCW.
(2) **Artifact creation.** During the workshop's artifact development (activity 2), participants will collaboratively create artifacts to reflect communal *commitments to action.* These artifacts will be made available to all workshop participants for future reference.
(3) **Publication of workshop proceedings.** Given the potentially sensitive nature of the R&R session, we will not publish workshop proceedings in a traditional sense but alternatively we will create a suite of scaffolding resources for other researchers to organize their own R&R workshops. This may include; our own reflections on what worked well and what could be improved, as well as discussion guides or templates for similar workshops. We will share these resources publicly across CSCW, HCI, and S&P communities.
(4) **Collective learning and community spirit.** The expert panel (activity 1) of this workshop is designed for panelists to

share their experiences and insights, and for all participants to collectively learn about the 'messiness' of sociotechnical safety research. Researchers will leave the workshop with learnings about pitfalls to avoid but with trusted mentors and peers to enable strategies for successfully reflexive research, and shared language.

## References


[1] Zainab Agha, Karla Badillo-Urquiola, and Pamela J. Wisniewski. 2023. "Strike at the Root": Co-designing Real-Time Social Media Interventions for Adolescent Online Risk Prevention. *Proc. ACM Hum.-Comput. Interact.* 7, CSCW1, Article 149 (apr 2023), 32 pages. doi:10.1145/3579625

[2] Rosanna Bellini, Emily Tseng, Noel Warford, Alaa Daffalla, Tara Matthews, Sunny Consolvo, Jill Palzkill Woelfer, Patrick Gage Kelley, Michelle L. Mazurek, Dana Cuomo, Nicola Dell, and Thomas Ristenpart. 2024. SoK: Safer Digital-Safety Research Involving At-Risk Users. IEEE Computer Society, 74–74. doi:10.1109/SP54263.2024.00071 ISSN: 2375-1207.

[3] Rasika Bhalerao, Vaughn Hamilton, Allison McDonald, Elissa M Redmiles, and Angelika Strohmayer. 2022. Ethical practices for security research with at-risk populations. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 546–553.

[4] Pernille Bjørn and Nina Boulus-Rødje. 2015. The multiple intersecting sites of design in CSCW research. *Computer Supported Cooperative Work (CSCW)* 24 (2015), 319–351.

[5] Lynn Weber Cannon. 1990. Fostering Positive Race, Class, and Gender Dynamics in the Classroom. *Women's Studies Quarterly* 18, 1/2 (1990), 126–134. jstor:40004032

[6] Periwinkle Doerfler, Andrea Forte, Emiliano De Cristofaro, Gianluca Stringhini, Jeremy Blackburn, and Damon McCoy. 2021. "I'm a Professor, which isn't usually a dangerous job": Internet-facilitated Harassment and Its Impact on Researchers. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (Oct. 2021), 341:1–341:32. doi:10.1145/3476082

[7] Brier Dudley. 2022. Harassment, public-records requests bombard UW truth seeker after Jan. 6 hearings cameo. https://www.seattletimes.com/opinion/harassment-public-records-requests-bombard-uw-truth-seeker-after-jan-6-hearings-cameo/

[8] Brianna Dym and Casey Fiesler. 2020. Social Norm Vulnerability and its Consequences for Privacy and Safety in an Online Community. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (Oct. 2020), 1–24. doi:10.1145/3415226

[9] KJ Kevin Feng, Rock Yuren Pang, Tzu-Sheng Kuo, Amy Winecoff, Emily Tseng, David Gray Widder, Harini Suresh, Katharina Reinecke, and Amy X Zhang. 2025. Sociotechnical AI Governance: Challenges and Opportunities for HCI. In *Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*. 1–6.

[10] Jessica L. Feuston, Arpita Bhattacharya, Nazanin Andalibi, Elizabeth A. Ankrah, Sheena Erete, Mark Handel, Wendy Moncur, Sarah Vieweg, and Jed R. Brubaker. 2022. Researcher Wellbeing and Best Practices in Emotionally Demanding Research. In *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems (CHI EA '22)*. Association for Computing Machinery, New York, NY, USA, 1–6. doi:10.1145/3491101.3503742

[11] Jessica L. Feuston, Arpita Bhattacharya, Nazanin Andalibi, Elizabeth A. Ankrah, Sheena Erete, Mark Handel, Wendy Moncur, Sarah Vieweg, and Jed R. Brubaker. 2022. Researcher Wellbeing and Best Practices in Emotionally Demanding Research. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts*. ACM, New Orleans LA USA, 1–6. doi:10.1145/3491101.3503742

[12] Eivind Flobak, Jo D Wake, Joakim Vindenes, Smiti Kahlon, Tine Nordgreen, and Frode Guribye. 2019. Participatory design of VR scenarios for exposure therapy. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.

[13] Douglas E Foley. 2002. Critical ethnography: The reflexive turn. *International journal of qualitative studies in education* 15, 4 (2002), 469–490.

[14] Paulo Freire. 2020. Pedagogy of the oppressed. In *Toward a sociology of education*. Routledge, 374–386.

[15] J George. 2017. Medical Morbidity and Mortality Conferences: Past, Present and Future. *Postgraduate Medical Journal* 93, 1097 (March 2017), 148–152. doi:10.1136/postgradmedj-2016-134103

[16] 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. *Proc. ACM Hum.-Comput. Interact.* 4, CSCW2, Article 124 (oct 2020), 27 pages. doi:10.1145/3415195

[17] Kata Issari. 2024. Lecture notes in SOC 582 Intimate Partner Violence & Trauma.

[18] Seny Kamara. 2020. Crypto for the People. Invited talk at CRYPTO.

[19] Tadayoshi Kohno, Yasemin Acar, and Wulf Loh. 2023. Ethical Frameworks and Computer Security Trolley Problems: Foundations for Conversations.

[20] Sarah Kuhn and Michael J Muller. 1993. Participatory design. *Commun. ACM* 36, 6 (1993), 24–29.

[21] Smita Kumar and Liz Cavallaro. 2018. Researcher Self-Care in Emotionally Demanding Research: A Proposed Conceptual Framework. *Qualitative Health Research* 28, 4 (March 2018), 648–658. doi:10.1177/1049732317746377

[22] Calvin Alan Liang, Emily Tseng, Akeiylah Dewitt, Yasmine Kotturi, Sucheta Ghoshal, Angela DR Smith, Marisol Wong-Villacres, Lauren Wilcox, and Sheena Erete. 2023. Surfacing Structural Barriers to Community-Collaborative Approaches in Human-Computer Interaction. In *Companion Publication of the 2023 Conference on Computer Supported Cooperative Work and Social Computing*. 542–546.

[23] Benedetta Lusi, Adrian K Petterson, Kamala Payyapilly Thiruvenkatanathan, Michaela Krawczyk, Emily Tseng, Lara Reime, Madeline Balaam, Katie A Siek, and Cristina Zaga. 2024. Caring for Reproductive Justice: Design in Response to Adversity. In *Companion Publication of the 2024 Conference on Computer-Supported Cooperative Work and Social Computing*. 693–696.

[24] Juan F Maestre, Elizabeth V Eikey, Mark Warner, Svetlana Yarosh, Jessica Pater, Maia Jacobs, Gabriela Marcu, and Patrick C Shih. 2018. Conducting research with stigmatized populations: Practices, challenges, and lessons learned. In *Companion of the 2018 ACM conference on computer supported cooperative work and social computing*. 385–392.

[25] Jessica McClearn, Rikke Bjerg Jensen, and Reem Talhouk. 2023. Othered, silenced and scapegoated: understanding the situated security of marginalised populations in Lebanon. In *32nd USENIX Security Symposium (USENIX Security 23)*. 4625–4642.

[26] 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.

[27] 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*. 1–14.

[28] Nora McDonald and Andrea Forte. 2021. Powerful privacy norms in social network discourse. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 1–27.

[29] Wendy Moncur. 2013. The emotional wellbeing of researchers: considerations for practice. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Paris France, 1883–1890. doi:10.1145/2470654.2466248

[30] Jay D. Orlander, Thomas W. Barber, and B. Graeme Fincke. 2002. The Morbidity and Mortality Conference: The Delicate Nature of Learning from Error. *Academic Medicine* 77, 10 (Oct. 2002), 1001.

[31] Morgan Klaus Scheuerman, Stacy M. Branham, and Foad Hamidi. 2018. Safe Spaces and Safe Places: Unpacking Technology-Mediated Experiences of Safety and Harm with Transgender People. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (Nov. 2018), 1–27. doi:10.1145/3274424

[32] Morgan Klaus Scheuerman, Alex Hanna, and Emily Denton. 2021. Do Datasets Have Politics? Disciplinary Values in Computer Vision Dataset Development. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (Oct. 2021), 317:1–317:37. doi:10.1145/3476058

[33] Morgan Klaus Scheuerman, Kandrea Wade, Caitlin Lustig, and Jed R. Brubaker. 2020. How We've Taught Algorithms to See Identity: Constructing Race and Gender in Image Databases for Facial Analysis. *Proceedings of the ACM on Human-Computer Interaction* 4 (May 2020), 58:1–58:35. doi:10.1145/3392866

[34] Yngve Sundblad. 2011. UTOPIA: Participatory design from Scandinavia to the world. In *History of Nordic Computing 3: Third IFIP WG 9.7 Conference, HiNC 3, Stockholm, Sweden, October 18-20, 2010, Revised Selected Papers 3*. Springer, 176–186.

[35] Reem Talhouk, Lizzie Coles-Kemp, Rikke Bjerg Jensen, Madeline Balaam, Andrew Garbett, Hala Ghattas, Vera Araujo-Soares, Balsam Ahmad, and Kyle Montague. 2020. Food aid technology: the experience of a Syrian refugee community in coping with food insecurity. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (2020), 1–25.

[36] Joice Tang, McKane Andrus, Samuel So, Udayan Tandon, Andrés Monroy-Hernández, Vera Khovanskaya, Sean A. Munson, Mark Zachry, and Sucheta Ghoshal. 2023. Back to "Back to Labor": Revisiting Political Economies of Computer-Supported Cooperative Work. In *Companion Publication of the 2023 Conference on Computer Supported Cooperative Work and Social Computing* (Minneapolis, MN, USA) *(CSCW '23 Companion)*. Association for Computing Machinery, New York, NY, USA, 522–526. doi:10.1145/3584931.3611285

[37] Emily Tseng, Rosanna Bellini, Yeuk-Yu Lee, Alana Ramjit, Thomas Ristenpart, and Nicola Dell. 2024. Data Stewardship in Clinical Computer Security: Balancing Benefit and Burden in Participatory Systems. *Proc. ACM Hum.-Comput. Interact.* 8, CSCW1, Article 39 (apr 2024), 29 pages. doi:10.1145/3637316

[38] Ashley Marie Walker, Michael Ann DeVito, Karla Badillo-Urquiola, Rosanna Bellini, Stevie Chancellor, Jessica L Feuston, Kathryn Henne, Patrick Gage Kelley, Shalaleh Rismani, Renee Shelby, et al. 2024. " What is Safety?": Building Bridges Across Approaches to Digital Risks and Harms. In *Companion Publication of the 2024 Conference on Computer-Supported Cooperative Work and Social Computing*.

736–739.
[39] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L. Mazurek, Manya Sleeper, and Kurt Thomas. 2022. SoK: A Framework for Unifying At-Risk User Research. In *2022 IEEE Symposium on Security and Privacy (SP)*. 2344–2360. doi:10.1109/SP46214.2022.9833643 ISSN: 2375-1207.
[40] Miranda Wei, Jaron Mink, Yael Eiger, Tadayoshi Kohno, Elissa M. Redmiles, and Franziska Roesner. 2024. SoK (or SoLK?): On the Quantitative Study of Sociodemographic Factors and Computer Security Behaviors. In *USENIX Security Symposium*. USENIX, Philadelphia, PA, USA.
[41] Alice Qian Zhang, Ryland Shaw, Jacy Reese Anthis, Ashlee Milton, Emily Tseng, Jina Suh, Lama Ahmad, Ram Shankar Siva Kumar, Julian Posada, Benjamin Shestakofsky, et al. 2024. The Human Factor in AI Red Teaming: Perspectives from Social and Collaborative Computing. In *Companion Publication of the 2024 Conference on Computer-Supported Cooperative Work and Social Computing*. 712–715.

## A Working Agreements

As a pre-workshop activity described in Section 3.1, we will circulate this initial list of working agreements, based on Ground Rules by Cannon [5] and adapted by Issari [17].

- We are here to learn together: to exchange ideas, to think critically, ask questions, dialogue, and pose solutions respectfully.
- We acknowledge that all forms of oppression exist and are likely to surface from time to time.
- We acknowledge that one aspect of institutionalized oppression is that we have systematically been taught misinformation about our own group and about members of other groups.
- We agree to actively pursue opportunities to learn new information that questions what we have been taught and to listen respectfully to unfamiliar perspectives.
- We agree not to blame ourselves or others for the misinformation we have learned, but to accept responsibility for not repeating misinformation after we have learned otherwise.
- We agree not to blame those that experience oppression for the condition of their lives.
- We agree that we will not demean, devalue, or in any way "put down" people for their experiences.
- We agree to actively challenge the myths and stereotypes about our own groups and other groups so that we can build our connections while also breaking down the walls that separate us.
- We want to create a comfortable atmosphere for open discussion. Anyone is welcome to ask that their comments not be repeated; please share other's personal information and/or comments only with their explicit consent.
- We embrace the differences and similarities among us, encouraging everyone to self-monitor to ensure all have equitable opportunity to participate. We challenge ourselves to communicate in new ways, including making time for silence, reflection, and processing.
- We agree to attend to our needs by nurturing ourselves mind, body and spirit.