Privacy and Power: Acknowledging the Importance of Privacy Research and Design for Vulnerable Populations

Nora McDonald
University of Maryland
Baltimore County
Baltimore, MD 21250, USA
nkm@umbc.edu

Karla Badillo-Urquiola
University of Central Florida
Orlando, FL 32826, USA
Kcurquiola10@knights.ucf.edu

Morgan G. Ames
University of California
Berkeley, CA, USA 94720
privacypower@morganya.org

Nicola Dell
Cornell Tech
New York, NY, USA 10044
nixdell@cornell.edu

Elizabeth Keneski
Facebook Research
Boston, MA
lizkenes@fb.com

Manya Sleeper
Google
Mountain View, CA
manya@google.com

Pamela J. Wisniewski
University of Central Florida
Orlando, FL 32826, USA
pamwis@ucf.edu

CHI'20 Extended Abstracts, April 25–30, 2020, Honolulu, HI, USA

ACM ISBN 978-1-4503-6819-3/20/04.
https://doi.org/10.1145/3334480.3375174

Abstract
Privacy researchers and designers must take into consideration the unique needs and challenges of vulnerable populations. Normative and privileged lenses can impair conceptualizations of identities and privacy needs, as well as reinforce or exacerbate power structures and struggles—and how they are formalized within privacy research methods, theories, designs, and analytical tools. The aim of this one-day workshop is to facilitate discourse around alternative ways of thinking about privacy and power, as well as ways for researching and designing technologies that not only respect the privacy needs of vulnerable populations but attempt to empower them. We will work towards developing best practices to help academics and industry folks, technologists, researchers, policy makers, and designers do a better job of serving the privacy needs of vulnerable users of technology.

Author Keywords
Vulnerable populations; intersectionality; privacy

CSS Concepts
• **Human-centered computing~HCI theory, concepts and models** • Security and privacy → Human and societal aspects of security and privacy

Some Problems and Questions for the CHI Community

- What identity research, design, and policies are necessary for vulnerable identities to thrive?
- How can research be structured to consider the ways in which privacy questions are shaped a priori by power structures?
- How can practice and design be developed/ rendered or evaluated (pre or post hoc) to understand how it perpetuates structures of power that are unfair to vulnerable identities?
- Are there ways that identities intersect to create added and more complex burdens? What are the burdens and risks? How can they be addressed?

Introduction

Vulnerable populations include, but are not limited to, survivors of domestic abuse [9], those living in poverty or within child welfare systems [3, 27], immigrants [11], those with HIV [29], LGBTQ [25], as well as the very young [31] and very old [13]. Populations we might define as vulnerable—those whose race, class, gender or sexual identity, and other intersectional characteristics or circumstances put them at particular risk in the society at large—are also made more susceptible to online privacy violations. Often, the privacy risks of vulnerable populations are not fully considered in the design of systems because those risks and potential harms are not fully understood (nor necessarily prioritized) by those responsible for research and design.

In our one-day workshop, we invite network privacy researchers, social justice researchers, and practitioners to work together to consider how vulnerable identities are disempowered and to interrogate the ways in which identities and power shape experiences of privacy. Our workshop aims to:

- Identify issues and challenges around "privacy and power" for vulnerable populations as it relates to both research and design practices.
- Consider the power dynamics that impact vulnerable privacy and how the addition of other methods and theories (e.g., intersectionality, queer-Marxism) helps to further tackle issues of power.

Privacy through the Lens of Intersectionality

At CHI 2018, our research community came together to acknowledge the importance of individual differences in privacy [30]. Our intention is to extend this discussion of privacy through the lens of intersectionality, specifically with its focus on structures of inequality and power. Despite the turn towards more intersectional Human-Computer Interaction (HCI) [8, 15, 22, 26, 28, 32], studies in our field (and more broadly in industry) tend to focus on a single attribute of struggle (rather than multiple identities) and (by implication) fail to see the power dynamics that coincide with their experience [24, 26]. For instance, it is not simply enough to consider race or color in a vacuum, rather we must also consider other identities, the power structures that shape individuals' subjectivity—how they believe others to see and think about them and therefore what privacy protections they are entitled to—and circumstances in ways that result in more harm. We want to bring this intersectionality lens to the networked privacy community to better understand and account for the unique privacy challenges of vulnerable populations.

Over the last half century, privacy research has evolved from leveraging individual-based theories (like Altman's boundary regulation [2]), to norm-based theories (like Nissenbaum's contextual integrity [19] or Petronio's communication privacy management Theory (CPM) [21]), to identity-based theories, like intersectionality [4, 5] that consider structures of inequality in relationship to compounding identities.

Identity-based theories and frameworks are useful for studying and designing for privacy with vulnerable populations because they are more attuned to the structural inequalities (i.e., power) that make some individuals more susceptible to privacy violations. They also help explain why violations of privacy may be more dire for vulnerable individuals.

Crenshaw argues that policies that assume a certain narrative about newcomers effectively ignore other dimensions of experience (structural discrimination in our laws, poverty, conditions of immigration, etc.) and systematically exclude people from entering [5]. Updated for the current privacy landscape, we can say that management of identity knowledge is always

Some Problems and Questions for the CHI Community, continued

- How do current designs consider vulnerable identities, if at all?
- What are some vulnerable users who might be harmed or hampered by the designs—e.g., intersections of gender, race or color, sexual identity, age (young and old) and domestic abuse survivors all of whom represent unique challenges for privacy researchers and designers?
- What are some unintended consequences of existing designs or technologies for vulnerable populations? How can we mitigate these harms? What can we learn from these cases?

limited by the scope of policy and tools that system designers make available and the social norms governing the situation. Intersectional identities create privacy challenges for individuals when, for instance, you are a poor, black mother, or a family in need of government assistance, with the obligation to disclose inappropriate information (e.g., about your sexual history) to secure benefits [7]. Surveillance of individuals disproportionately harms vulnerable and low-income (intersectional) populations just for taking part in society. For low-income communities, surveillance can lead to avoidance of financial and social institutions for whom the risks of privacy breaches are greater because they lack secure technologies and resources for combating privacy violations like identity theft [17].

In summary, there are great challenges we face adapting general concepts of privacy in the face of rapidly changing networked information technologies. Moreover, vulnerable populations experience privacy risks *even more keenly* because their status creates additional vulnerabilities whose implications may extend to all aspects of their lives including their personal liberty. It is therefore imperative that the SIGCHI community consider how intersectionality and power play a key role in privacy research and design.

Workshop Themes

The first theme of our workshop focuses on defining "privacy and power" (or the lack thereof) and identifying broad challenges within related research and design practices. How can researchers and designers *reconcile power* within privacy research, design, and practice? Our second theme explores the power dynamics that impact vulnerable privacy and how the addition of other methods and theories helps to further tackle issues of power (e.g., intersectionality, politics and identity and political economies [6]).

Theme 1: Identifying the challenges around privacy and power for vulnerable *populations*

Often vulnerable experiences coincide with conditions brought on by structural inequalities and social norms (of discrimination and that are permissive of it). These scenarios may be challenging for designers and technologists to understand and grapple with—precisely because of the normative lens they have. But if designers and technologists can't examine how power is rendered in existing designs, can't imagine vulnerable users, and don't seek them out during all phases of research and design, then vulnerable identities will be left out of privacy design and policy. For example, in the area of online safety for teens, there are power imbalances between teens and parents concerning privacy, safety, and autonomy. Current technologies designed for keeping teens safe online focus on parental control, rather than teen self-regulation. Researchers are attempting to move towards more teen-centered solutions that are more respectful of their privacy and empower teens to protect themselves online [3, 31]. However, researchers and designers are not just thinking in terms of vulnerable identities to shape (or at very least, inform) research and decision-making, they are also moving to incorporate youth into their research and design practices and thinking, and specifically with consideration for power dynamics and structures. Similarly, Marwick et al. use participant researchers in their study of privacy for low socioeconomic young adults [18]. We pose some key questions around privacy and power that consider how researchers and designs might integrate vulnerable identities into their research and design practices (see side bar).

Theme 2: Identifying Theories, Research Methods, and Design Practices to Tackle the Challenges around Privacy and Power for Vulnerable Populations

For our second theme, we believe privacy researchers and designers can leverage methods and theories to

Previous CHI/CSCW Workshops on Privacy

- **CHI 2011**: Privacy for a Networked World: Bridging Theory and Design
- **CSCW 2012**: Reconciling
- Privacy with Social Media
- **CSCW 2013**: Measuring
- Networked Social Privacy
- **CSCW 2015**: The Future of Networked Privacy: Challenges and Opportunities
- **CHI 2016**: Bridging the Gap Between Privacy by Design and Privacy in Practice
- **CSCW 2017**: In Whose Best Interest? Exploring the Real, Potential, and Imagined Ethical Concerns in Privacy-Focused Agenda
- **CHI 2018**: Moving Beyond a 'One-size fits all' Approach: Exploring Individual Differences in Privacy
- **CSCW 2018**: Privacy in Context: Critically Engaging with Theory to Guide Privacy Research and Design
- **CSCW 2019**: Ubiquitous Privacy: Research and Design for Mobile and IoT Platforms

enhance the intersectional theories' interrogation of power. Therefore, we pose the following question: *What theories, methods, and design practices should we leverage for intersectional privacy research and design?*

Theories

Existing privacy research frameworks, including individual (e.g., boundary regulation [2]), norm-based (e.g., contextual integrity [19]), and privacy/digital literacy (e.g., [12, 20]) theories, often do not provide mechanisms for considering vulnerabilities (e.g., class- or race-based struggles) and, instead, should be intersectional in their approach (i.e., consider those identities in multiplicity and in relation to power). Therefore, we plan to introduce privacy researchers to intersectional and queer-Marxist theory, and to encourage researchers and designers to consider the themes outlined by anarchic HCI [14]. Queer-Marxist theory invokes material struggles and is thus relevant for vulnerable communities who are made more vulnerable because of economic circumstances [16]. Moreover, alongside intersectionality, queer-Marxist theory offers a critical lens through which to examine identity and class as not in opposition to norms so much as how they operate.

Empirical Methods

Researchers and designers have begun to focus on sampling and privileging the voices of intersectional identities in *all* design—from requirements gathering, to ideation, to implementation and testing, and ultimately policy-making. Scholars should also consider ways to interrogate the very systems they study with methods like critical discourse analysis (CDA). CDA is a useful lens through which to look at language relative to social, political, and cultural formations [23] and we are encouraged by scholars who are trying to update this practice to interrogate design as discourse.

Design Practices

Designing for vulnerable users' privacy not only involves understanding individual perceptions of risk, but also the power structures that perpetuate these conditions in the first place. This requires that we radically rethink representation on social media as well as forms of participation that support different kinds of privacy. For example, intimate partner violence (IPV) defies typical threat models because abusers often have access to victims' phones and can carry out injurious, albeit unsophisticated attacks by directly accessing their devices and information, rather than through installing malicious software [10]. The challenges for IPV victims are a useful analog to the broader problems for privacy and security, which is that threats are highly individual and so are the specific mitigation strategies that individuals at risk must employ to counter them. Freed et al. thus argue that we should use IPV as the starting point for privacy design [10].

Workshop Goals

Building upon past ACM CHI and CSCW networked privacy workshops (listed in the sidebar), our goal is to facilitate conversations about privacy discourse and practice in respect to vulnerable populations and which turn our focus usefully (effectively) to power. By bringing together privacy researchers and designers, we hope to encourage collaborative efforts across disciplines that emphasize respect for the privacy needs of vulnerable populations. Ultimately, it is our goal to deliver best practices to the broader HCI community in hopes of broadening their perspectives on intersectional privacy research and design.

Workshop Organizers

Nora McDonald is a Post-doctoral researcher at UMBC with a PhD in Information Science from Drexel University. Her work focuses on privacy for vulnerable

Program Committee

- Louise Barkuus
- Foad Hamidi
- Oliver Haimson
- Roberto Hoyle
- Jen King
- Lorraine Kisselburgh
- Priya Kumar
- Airi Lampinen
- Damon McCoy
- Helena Mentis
- Vivian Motti
- Xinru Page
- Chanda Phelan
- Afsaneh Razi
- Florian Schaub
- Luke Stark
- Yang Wang
- Yaxing Yao
- Michael Zimmer

Workshop Panelists

As experts in the areas of privacy and/or vulnerable populations, the workshop co-organizers will host a panel and Q & A session during the workshop.

- Nora McDonald
- Morgan Ames
- Nicola Dell
- Tamy Guberek
- Manya Sleeper
- Pamela J. Wisniewski (panel moderator)

populations and, more broadly, on social justice and technology design.

Karla Badillo-Urquiola is a PhD candidate and McKnight Doctoral Fellow in Modeling and Simulation at the University of Central Florida. She leverages her interdisciplinary background to investigate online safety and privacy for teens in the foster care system.

Morgan G. Ames is an Assistant Adjunct Professor in the School of Information at the University of California, Berkeley. Her book *The Charisma Machine: The Life, Death, and Legacy of One Laptop per Child* (MIT Press, 2019) explores the cultural history, results, and legacy of the OLPC project.

Nicola Dell is an Assistant Professor at Cornell Tech and the Jacobs Technion Cornell Institute. She focuses on designing, building, and evaluating novel computing systems that improve the lives of underserved populations in the US and around the world.

Elizabeth Keneski directs privacy research at Facebook where she is focused on offline and online privacy experiences and user mental models. She has a PhD in Social Psychology from The University of Texas Austin.

Manya Sleeper is a user experience researcher at Google focused on usable security and privacy. She has a PhD in Societal Computing from Carnegie Mellon University.

Pamela J. Wisniewski is an Assistant Professor in the Department of Computer Science at the University of Central Florida. Her research expertise is situated at the juxtaposition of Social Computing and Privacy with an emphasis on adolescent online safety.

Workshop Website

The website for the workshop is networkedprivacy2020.wordpress.com, which will be linked from the Networked Privacy community's permanent website: networkedprivacy.com. All information related to the workshop (e.g., call for participation, important dates, schedule) will be available on the website. Once participants have been selected, the website will also host the accepted position papers.

Pre-Workshop Plans

Workshop participants will be recruited from the SIGCHI community, previous CHI and CSCW privacy workshops, and the organizers' extended research networks. To ensure a balanced mix of participants from HCI, design, social sciences, and other interdisciplinary fields, we will recruit participants via social media, social media groups (e.g., CHIMeta, CSCWMeta, CRA-WP), email list-servs, and appropriate community boards. These efforts will also be supported by the workshop's program committee (see side panel).

Workshop Structure

The workshop will be structured to facilitate conversation around privacy and power. We encourage participants to propose case studies and thoughtful probes in addition to those the workshop organizers propose to support our discussion of themes.

1. **Welcome/Introductions:** The organizers will present the schedule and goals of the workshop to the participants and facilitate brief introductions.
2. **Lightning talks:** Presentation of privacy and power position papers accepted to the workshop.
3. **Large Group Discussion:** Participants will identify the most pressing challenges in intersectionality research and design.
4. **Coffee Break**

5. **Panel Discussion:** Privacy scholars and Social Justice Scholars will engage the audience in a discussion of themes around vulnerable privacy and power. For panel participants see sidebar.
6. **Lunch**
7. **Break-out activity:** Participants will breakout into small groups to discuss challenges, processes, etc. based on the themes: either issues and challenges around "privacy and power" for vulnerable populations OR how the addition of other methods and theories (e.g., intersectionality, queer-Marxism) helps to further tackle issues of power for vulnerable populations.
8. **Reporting Outcomes:** Each small group will report back their ideas. As a large group, everyone will work together to synthesize ideas and strengthen the proposed guiding principles.
9. **Next Steps:** The workshop will end with a large group discussion on opportunities for further collaboration between participants. We will discuss concrete ways to engage the HCI community in research that addresses power.

The goals and planned outcomes for this workshop include: (1) documentation of the important challenges and open questions concerning the privacy of vulnerable populations and power in HCI; (2) documentation of brainstorming towards interrogating power and best practices; and (3) planning for engaging the HCI community with these issues during and after the conference.

Post-Workshop Plans

After the workshop, the organizers will report the outcomes on a blog post [1]. A digital copy of this report will later be emailed to workshop participants as well as uploaded to the workshop website. Additional outputs like articles in other publishing venues will be explored by the workshop organizers.

Call for Participation

We encourage workshop participants to submit a position paper that probes tensions around HCI privacy research and power for vulnerable identities, as well as how to overcome them through intersectional methodology and research design. Importantly, we encourage privacy research who have not previously conducted research or designed for vulnerable populations to attend this workshop.

Participants will be required to submit a 2-4 page position paper in the SIGCHI extended abstract format. Submissions can be structured in multiple ways: (1) a discussion of a specific themes we propose or (2) a case study discussion of a specific experience regarding the study of vulnerable populations, particularly how authors dealt with interrogating or addressing issues of privacy and power. We encourage submissions that are honest and subversive. Note that participants need not have prior experience with this type of work. We invite and encourage submissions from researchers from academia, industry, non-profits, and governments (national, regional, local, Tribal), and welcome a wide range of disciplinary perspectives.

Papers will be peer-reviewed by the program committee (see sidebar), and submissions will be accepted based on the quality of the position paper, relevance and engagement to the workshop themes, as well as the participant's potential to meaningfully contribute to the workshop discussions and goals.

Workshop papers should be emailed to networkedprivacy2020@gmail.com. At least one author of each accepted position paper must attend the workshop. All participants must register for both the workshop and for at least one day of the conference. For more information, visit networkedprivacy2020.wordpress.com.

References

[1] A Review of the CSCW 2018 "Privacy in Context" Workshop: 2019. *https://medium.com/acm-cscw/a-review-of-the-cscw-2018-privacy-in-context-workshop-ae380040f1ec*. Accessed: 2019-09-30.

[2] Altman, I. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Brooks/Cole.

[3] Badillo-Urquiola, K., Page, X. and Wisniewski, P. 2019. Risk vs. Restriction: The Tension between Providing a Sense of Normalcy and Keeping Foster Teens Safe Online. *The ACM CHI Conference on Human Factors in Computing Systems* (2019).

[4] Crenshaw, K. 1989. Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine. *University of Chicago Legal Forum*. 1989, 1 (1989).

[5] Crenshaw, K. 1991. Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color. *Stanford Law Review*. 43, 6 (1991), 1241–1299.

[6] Ekbia, H. and Nardi, B. 2016. Social Inequality and HCI: The View from Political Economy. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2016), 4997–5002.

[7] Eubanks, V. 2018. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press.

[8] Fox, S., Menking, A., Steinhardt, S., Hoffmann, A.L. and Bardzell, S. 2017. Imagining Intersectional Futures: Feminist Approaches in CSCW. *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (New York, NY, USA, 2017), 387–393.

[9] Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T. and Dell, N. 2018. A Stalker's Paradise: How Intimate Partner Abusers Exploit Technology. (2018), 1–13.

[10] Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T. and Dell, N. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. (2018), 1–13.

[11] Guberek, T., McDonald, A., Simioni, S., Mhaidli, A.H., Toyama, K. and Schaub, F. 2018. Keeping a Low Profile?: Technology, Risk and Privacy Among Undocumented Immigrants. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2018), 114:1–114:15.

[12] Hargittai, E. 2005. Survey Measures of Web-Oriented Digital Literacy. *Social Science Computer Review*. 23, 3 (2005), 371–379.

[13] Hornung, D., Müller, C., Shklovski, I., Jakobi, T. and Wulf, V. 2017. Navigating Relationships and Boundaries: Concerns Around ICT-uptake for Elderly People. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2017), 7057–7069.

[14] Keyes, O., Hoy, J. and Drouhard, M. 2019. Human-Computer Insurrection: Notes on an Anarchist HCI. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2019), 339:1–339:13.

[15] Kumar, N. and Karusala, N. 2019. Intersectional Computing. *Interactions*. 26, 2 (Feb. 2019), 50–54.

[16] Lewis, H. 2016. *The Politics of Everybody: Feminism, Queer Theory and Marxism at the Intersection*. Zed Books.

[17] Madden, M., Gilman, M., Levy, K. and Marwick, A. 2017. Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans. *Washington University Law Review*. 95, 1 (Jan. 2017), 053–125.

[18] Marwick, A., Fontaine, C. and boyd, danah 2017. "Nobody Sees It, Nobody Gets Mad": Social Media, Privacy, and Personal Responsibility Among Low-SES Youth. *Social Media + Society*. 3, 2 (Apr. 2017).

[19] Nissenbaum, H. 2010. *Privacy in context: technology, policy, and the integrity of social life*. Stanford Law Books.

[20] Park, Y.J. 2011. Digital Literacy and Privacy Behavior Online. *Communication Research*. 40, 2 (2011), 215–236.

[21] Petronio, S.S. 2002. *Boundaries of privacy: dialectics of disclosure*. State University of New York Press.

[22] Rankin, Y.A. and Thomas, J.O. 2019. Straighten Up and Fly Right: Rethinking Intersectionality in HCI Research. *Interactions*. 26, 6 (Oct. 2019), 64–68.

[23] Rogers, R., Malancharuvil-Berkes, E., Mosley, M., Hui, D. and Joseph, G.O. 2005. Critical Discourse Analysis in Education: A Review of the Literature. *Review of Educational Research*. 75, 3 (2005), 365–416.

[24] Rogue, J. and Volcano, A. 2012. Insurrection at the intersections: Feminism, intersectionality, and anarchism. *Quiet rumors: An anarcha-feminist reader*. AK Press. 43–46.

[25] Scheuerman, M.K., Branham, S.M. and Hamidi, F. 2018. Safe Spaces and Safe Places: Unpacking Technology-Mediated Experiences of Safety and Harm with Transgender People. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW (Nov. 2018), 155:1–155:27.

[26] Schlesinger, A., Edwards, W.K. and Grinter, R.E. 2017. Intersectional HCI: Engaging Identity Through Gender, Race, and Class. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2017), 5412–5427.

[27] Sleeper, M., Matthews, T., O'Leary, K., Turner, A., Woelfer, J.P., Shelton, M., Oplinger, A., Schou, A. and Consolvo, S. 2019. Tough Times at Transitional Homeless Shelters: Considering the Impact of Financial Insecurity on Digital Security and Privacy. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2019), 89:1–89:12.

[28] Thomas, J.O., Joseph, N., Williams, A., Crum, C. and Burge, J. 2018. Speaking Truth to Power: Exploring the Intersectional Experiences of Black Women in Computing. *2018 Research on Equity and Sustained Participation in Engineering, Computing, and Technology (RESPECT)* (Feb. 2018), 1–8.

[29] Warner, M., Gutmann, A., Sasse, M.A. and Blandford, A. 2018. Privacy Unraveling Around Explicit HIV Status Disclosure Fields in the Online Geosocial Hookup App Grindr. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW (Nov. 2018), 181:1–181:22.

[30] Wilkinson, D., Namara, M., Badillo-Urquiola, K., Wisniewski, P.J., Knijnenburg, B.P., Page, X., Toch, E. and Romano-Bergstrom, J. 2018. Moving Beyond a "One-size Fits All": Exploring Individual Differences in Privacy. *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2018), W16:1–W16:8.

[31] Wisniewski, P., Ghosh, A.K., Xu, H., Rosson, M.B. and Carroll, J.M. 2017. Parental Control vs. Teen Self-Regulation: Is There a Middle Ground for Mobile Online Safety? *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (New York, NY, USA, 2017), 51–69.

[32] Wisniewski, P.J., Kumar, N., Bassem, C., Clinch, S., Dray, S.M., Fitzpatrick, G., Lampe, C., Muller, M. and Peters, A.N. 2018. Intersectionality As a Lens to Promote Equity and Inclusivity Within SIGCHI. *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2018).