Where are Marginalized Communities in Cybersecurity Research?

Anadi Chattopadhyay
Swarthmore College

Rodrigo Carvajal
Swarthmore College

Vasanta Chaganti
Swarthmore College

Sukrit Venkatagiri
Swarthmore College

Abstract

Marginalized communities are disproportionately vulnerable to cybersecurity threats, but are rarely the focus of inquiry in cybersecurity research. In this paper, we systematically analyzed recent security, privacy, and cybersecurity publications to understand the frequency and nature of engagement with marginalized communities by reviewing papers across four different professional societies' venues (ACM, IEEE, USENIX, and PoPETS) published in the last two years. Of 2,170 papers, we find that only 0.2% (27) of papers engage with marginalization in any form, with the majority of papers (22) being observational studies, and only five that included an intervention to actively support a marginalized community. We discuss how cybersecurity research can make strides towards not only understanding but also actively supporting marginalized groups.

1 Introduction and Related Work

Marginalized communities are especially vulnerable to cybersecurity attacks because of two factors: (1) reduced access to technical, socioeconomic, and legal support [8, 10, 31]; and (2) distrust of institutions from prior negative interactions [6, 29]. Simultaneously, these two factors make marginalized groups less able to recover from attacks such as identity theft, financial loss, and reputational damage, among others [23]. Recently, Sannon and Forte [21] analyzed research published from 2010 to 2020 to understand how marginalization is discussed in privacy research (not security) and found that only 3% of papers included a marginalized context. In our work we use the term "marginalization" to refer to *systematic, intentional, or unintentional exclusion or discrimination of individuals or groups based on: a facet of their identity as it relates to access to technology or methods for supporting their security and privacy on digital devices and platforms*. For example, with respect to age, race, nationality, gender, sexual orientation, socioeconomic status, and geographic location. Marginalization affects both adults and younger individuals, and can be extenuated by educational barriers, health disparities, and social developmental challenges.

In our literature review we shortlisted 2,170 papers published in the last two years in relevant scholarly libraries and security and privacy (S&P) conference venues (discussed below). Engaging with literature on marginalization and examining this dataset, we derived a novel framework to categorize each paper to answer two key research questions: **RQ1:** How do researchers define "marginalization" in the context of cybersecurity research? and **RQ2:** What methods are used to engage with, study, or support marginalized groups?

Our rationale for RQ1 and RQ2 was to understand what groups are prioritized by the S&P community and how researchers conceptualize and operationalize marginalization. We additionally wanted to understand what problem areas researchers seek to address, if researchers are actually engaging with marginalized communities, and what methodological approaches they use.

In this work we make three contributions. First, we understand how papers published in the last two years consider marginalization not only in terms of *privacy*, but also *security* and *cybersecurity*. Second, we contribute a large-scale comparative analysis of the *methods* used across all papers published in these two years across four different professional societies' venues (ACM, IEEE, USENIX, and PoPETs). Third, we categorize and contextualize papers focused on addressing marginalization in cybersecurity research. If researchers hope to make meaningful strides towards safe and productive digital spaces, there must be a greater emphasis on understanding and designing interventions to support marginalized communities.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.
August 11–13, 2024, Philadelphia, PA, United States.

2 Methods

Data Collection and Processing. We searched five relevant libraries/venues that have conferences and journals related to security, privacy, and cybersecurity: The ACM Digital Library, SOUPS (Symposium on Usable Privacy and Security), USENIX (Unix Users Group), PoPETS (Proceedings on Privacy Enhancing Technologies Symposium), and IEEE (Institute of Electrical and Electronics Engineers). To ensure that our dataset contained relevant papers, our search terms were "privacy", "security", "cyber", and "cybersecurity", and we restricted our search to the title and abstract of papers. From the resulting dataset, we examined papers published in the last two full years (2022 and 2023). We then created a standardized dataset with the same metadata across all venues. After removing duplicates we were left with 2,170 papers in our dataset: 1,705 papers from ACM, 40 from SOUPS, 98 from USENIX, 100 from PoPETS, and 228 papers from IEEE.

Data Analysis. After we arrived at our definition for marginalization described in Section 1, two authors coded a subset of the dataset based on our research questions along three dimensions: (1) whether or not the paper concerned marginalized communities (RQ1), (2) methodology used in the paper (RQ2), and (3) whether or not marginalized communities were supported or studied in the research (RQ2).

To answer RQ2, we coded papers based on its primary focus and methodology: (1) Theoretical, (2) Empirical, (3) System/Algorithm Design, and (4) People. *Theoretical* papers included those that developed or discussed new conceptual frameworks, theories or models relating to S&P, as well as literature reviews with findings. *Empirical* papers employed quantitative methods, such as experiments or mathematical analyses, to collect and analyze data, or qualitative methods such as observation, focus groups, or content analysis, to gather and interpret data on S&P. *System/Algorithm Design* papers involved the design or development of new systems, algorithms, or prototypes that were looking to enhance S&P. *People* focused papers involved directly interacting with individuals or groups through methods such as user centered design, community-based research, and interviews; i.e. the papers with community engagement and collaboration.

3 Findings

Of 2,170 papers collected, only 27 (0.2%) centered marginalized communities. Many of these 27 papers shared four commonalities across: (1) communities studied/worked with, (2) methods used, (3) type of intervention, and (4) results.

Communities Studied/Worked With. For RQ1, the majority of papers considered marginalization along lines of (dis)ability and socioeconomic status (SES): nine papers were about people with physical or learning disabilities [3, 13, 14, 15, 20, 27, 28, 33, 34] and five papers were about people from low-SES backgrounds [4, 5, 17, 18, 32]. The remaining 13 papers were with/about one or more of the following groups: survivors of intimate partner violence [9, 25, 30] or supporters of survivors [26], women [2, 7], LGBTQ+ people [12, 16], immigrants/refugees [1, 16], students that may have included individuals from marginalized backgrounds [24], and people in the Global South [22]. None of the 27 papers solely considered race as an element of marginalization.

Methods Used. For RQ2, we observed that many of the papers that were about marginalized communities predominantly used two methods for their research. The first, Data Analysis papers, were those that utilize statistical tools to come about solutions, and findings, focusing on the analysis of large datasets or longitudinal studies [9, 14, 15, 25, 32]. The second, Interviews, were the most common qualitative research method used at 15 papers. These studies provided a more in-depth understanding of the specific challenges and viewpoints of these communities [2, 3, 4, 5, 7, 11, 12, 17, 18, 20, 22, 26, 28, 33, 34].

Type of Intervention. For RQ2, we identified two areas in which papers that support marginalized communities fall under: Interventions and Evidence-Based Practices. Interventions refer to when the researchers successfully implement and evaluate security and privacy measures for marginalized communities. Several papers in our dataset employed these interventions [16, 24, 30]. Other papers employed Evidence-Based Practices that have empirically shown to enhance security accessibility for marginalized groups [3, 7, 17].

Results. Most papers detailed the importance of tailoring cybersecurity to the unique needs of their marginalized communities. Seven papers presented frameworks that proposed theoretical solutions to support the creation of more accessible and equitable security systems [4, 14, 16, 17, 19, 27, 28]. Similarly, four papers presented inclusive security designs that were either synthesized or theorized [1, 7, 24, 30], showcasing practices and principles that aim to make cybersecurity more accessible for individuals from marginalized or vulnerable communities.

4 Discussion and Conclusion

In this short paper, we synthesized a definition of marginalization centered around cybersecurity, introduced a novel framework to analyze papers, and highlighted methodological trends in S&P research. Our analysis of 27 papers published in the last two years across five venues highlights a dearth of research that actively supports marginalized communities. We also found a lack of investigation into racial factors and a tendency for researchers to continue creating frameworks for further study rather than making contributions themselves. If researchers hope for equitable social advancement in the digital world, we must strive to not only understand but also actively support marginalized communities through close-knit and long-term collaboration.

Acknowledgments

We would like to thank Shruti Sannon as well as members of the Collective Resilience Lab for their assistance. This work was supported by the National Science Foundation (NSF) under SaTC Award CNS-2348326 and a Google Award for Inclusion Research. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the NSF or Google.

References

[1] Ruba Abu-Salma, Reem Talhouk, Jose Such, Claudia Aradau, Francesca Meloni, Shijing He, Syed Ishtiaque Ahmed, Cansu Ekmekcioglu, Dina Sabie, Rikke Bjerg Jensen, Jessica McClearn, Anne Weibert, Max Kr¨uger, Faheem Hussain, and Rehema Baguma. Diverse migration journeys and security practices: Engaging with longitudinal perspectives of migration and (digital) security. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI EA '23, New York, NY, USA, 2023. Association for Computing Machinery.

[2] Tanisha Afnan, Yixin Zou, Maryam Mustafa, Mustafa Naseem, and Florian Schaub. Aunties, strangers, and the fbi: online privacy concerns and experiences of muslim-american women. In *Proceedings of the Eighteenth USENIX Conference on Usable Privacy and Security*, SOUPS'22, USA, 2022. USENIX Association.

[3] Taslima Akter, Tousif Ahmed, Apu Kapadia, and Manohar Swaminathan. Shared privacy concerns of the visually impaired and sighted bystanders with camera-based assistive technologies. *ACM Trans. Access. Comput.*, 15(2), may 2022.

[4] Wael S Albayaydh and Ivan Flechais. Exploring bystanders' privacy concerns with smart homes in jordan. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. Association for Computing Machinery.

[5] Laura Benton, Asimina Vasalou, and Sarah Turner. Location, location, security? exploring location-based smart device security concerns and mitigations within low-rent homes. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference*, DIS '23, page 1060–1077, New York, NY, USA, 2023. Association for Computing Machinery.

[6] Tiffany N. Brannon. Pride-and-prejudice perspectives of marginalization can advance science and society. *Current Directions in Psychological Science*, 32(1):73–80, 2023.

[7] George Hope Chidziwisano and Maureen Jalakasi. Understanding women's perspectives on smart home security systems in patriarchal societies of malawi. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference*, DIS '23, page 1078–1092, New York, NY, USA, 2023. Association for Computing Machinery.

[8] Munmun De Choudhury, Sachin R. Pendse, and Neha Kumar. Benefits and harms of large language models in digital mental health, 2023.

[9] Alaa Daffalla, Marina Bohuk, Nicola Dell, Rosanna Bellini, and Thomas Ristenpart. Account security interfaces: important, unintuitive, and untrustworthy. In *Proceedings of the 32nd USENIX Conference on Security Symposium*, SEC '23, USA, 2023. USENIX Association.

[10] Michael A Devito, Ashley Marie Walker, Jeremy Birnholtz, Kathryn Ringland, Kathryn Macapagal, Ashley Kraus, Sean Munson, Calvin Liang, and Herman Saksono. Social technologies for digital wellbeing among marginalized communities. In *Companion Publication of the 2019 Conference on Computer Supported Cooperative Work and Social Computing*, pages 449–454, 2019.

[11] Kelsey R. Fulton, Samantha Katcher, Kevin Song, Marshini Chetty, Michelle L. Mazurek, Chloé Messdaghi, and Daniel Votipka. Vulnerability discovery for all: Experiences of marginalization in vulnerability discovery. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 1997–2014, 2023.

[12] Christine Geeng, Mike Harris, Elissa Redmiles, and Franziska Roesner. "like lesbians walking the perimeter": Experiences of U.S. LGBTQ+ folks with online security, safety, and privacy advice. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 305–322, Boston, MA, August 2022. USENIX Association.

[13] Felicia Hellems and Sajal Bhatia. Removing the veil: Shining light on the lack of inclusivity in cybersecurity education for students with disabilities. In *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education V. 2*, SIGCSE 2022, page 1108, New York, NY, USA, 2022. Association for Computing Machinery.

[14] Elaine Lau and Zachary Peterson. A research framework and initial study of browser security for the visually impaired. In *Proceedings of the 32nd USENIX Conference on Security Symposium*, SEC '23, USA, 2023. USENIX Association.

[15] Brittany Lewis, Tina-Marie Ranalli, Alexandra Gourley, Piriyankan Kirupaharan, and Krishna Venkatasubramanian. "i... caught a person casing my house... and scared him off:" the use of security-focused smart home devices by people with disabilities. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, New York, NY, USA, 2023. Association for Computing Machinery.

[16] Jessica McClearn, Rikke Bjerg Jensen, and Reem Talhouk. Othered, silenced and scapegoated: understanding the situated security of marginalised populations in lebanon. In *Proceedings of the 32nd USENIX Conference on Security Symposium*, SEC '23, USA, 2023. USENIX Association.

[17] Maryam Mustafa, Abdul Moeed Asad, Shehrbano Hassan, Urooj Haider, Zainab Durrani, and Katharina Krombholz. Pakistani teens and privacy - how gender disparities, religion and family values impact the privacy design space. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, CCS '23, page 195–209, New York, NY, USA, 2023. Association for Computing Machinery.

[18] Sheza Naveed, Hamza Naveed, Mobin Javed, and Maryam Mustafa. "ask this from the person who has private stuff": Privacy perceptions, behaviours and beliefs beyond w.e.i.r.d. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. Association for Computing Machinery.

[19] Luke E. Richards, Edward Raff, and Cynthia Matuszek. Measuring equality in machine learning security defenses: A case study in speech recognition. In *Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security*, AISec '23, page 161–171, New York, NY, USA, 2023. Association for Computing Machinery.

[20] Jessica N. Rocheleau and Sonia Chiasson. Privacy and safety on social networking sites: Autistic and non-autistic teenagers' attitudes and behaviors. *ACM Trans. Comput.-Hum. Interact.*, 29(1), jan 2022.

[21] Shruti Sannon and Andrea Forte. Privacy research with marginalized groups: What we know, what's needed, and what's next. *Proc. ACM Hum.-Comput. Interact.*, 6(CSCW2), nov 2022.

[22] Ankit Shrestha, Tanusree Sharma, Pratyasha Saha, Syed Ishtiaque Ahmed, and Mahdi Nasrullah Al-Ameen. A first look into software security practices in bangladesh. *ACM J. Comput. Sustain. Soc.*, 1(1), sep 2023.

[23] Mattea Sim, Kurt Hugenberg, Tadayoshi Kohno, and Franziska Roesner. A scalable inclusive security intervention to center marginalized & vulnerable populations in security & privacy design. In *Proceedings of the 2023 New Security Paradigms Workshop*, pages 102–115, 2023.

[24] Mattea Sim, Kurt Hugenberg, Tadayoshi Kohno, and Franziska Roesner. A scalable inclusive security intervention to center marginalized & vulnerable populations in security & privacy design. In *Proceedings of the 2023 New Security Paradigms Workshop*, NSPW '23, page 102–115, New York, NY, USA, 2023. Association for Computing Machinery.

[25] Julia Slupska and Megan Lindsay Brown. Aiding intimate violence survivors in lockdown: Lessons about digital security in the covid-19 pandemic. In *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI EA '22, New York, NY, USA, 2022. Association for Computing Machinery.

[26] Julia Slupska and Angelika Strohmayer. Networks of care: Tech abuse advocates' digital security practices. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 341–358, Boston, MA, August 2022. USENIX Association.

[27] Abigale Stangl, Emma Sadjo, Pardis Emami-Naeini, Yang Wang, Danna Gurari, and Leah Findlater. "dump it, destroy it, send it to data heaven": Blind people's expectations for visual privacy in visual assistance technologies. In *Proceedings of the 20th International Web for All Conference*, W4A '23, page 134–147, New York, NY, USA, 2023. Association for Computing Machinery.

[28] Abigale Stangl, Kristina Shiroma, Nathan Davis, Bo Xie, Kenneth R. Fleischmann, Leah Findlater, and Danna Gurari. Privacy concerns for visual assistance technologies. *ACM Trans. Access. Comput.*, 15(2), may 2022.

[29] Jordan Taylor, Ellen Simpson, Anh-Ton Tran, Jed R. Brubaker, Sarah E Fox, and Haiyi Zhu. Cruising queer hci on the dl: A literature review of lgbtq+ people in hci. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, CHI '24, New York, NY, USA, 2024. Association for Computing Machinery.

[30] Emily Tseng, Mehrnaz Sabet, Rosanna Bellini, Harkiran Kaur Sodhi, Thomas Ristenpart, and Nicola Dell. Care infrastructures for digital security in intimate partner violence. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. Association for Computing Machinery.

[31] Aditya Vashistha, Richard Anderson, and Shrirang Mare. Examining security and privacy research in developing regions. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies*, pages 1–14, 2018.

[32] Victor Yisa, Reza Ghaiumy Anaraky, Bart Knijnenburg, and Rita Orji. Investigating privacy decision-making processes among nigerian men and women. *Proceedings on Privacy Enhancing Technologies*, 2023:294–308, 01 2023.

[33] Y. Yu, S. Ashok, S. Kaushik, Y. Wang, and G. Wang. Design and evaluation of inclusive email security indicators for people with visual impairments. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 2885–2902, Los Alamitos, CA, USA, may 2023. IEEE Computer Society.

[34] Yuhang Zhao, Yaxing Yao, Jiaru Fu, and Nihan Zhou. "if sighted people know, i should be able to know": privacy perceptions of bystanders with visual impairments around camera-based technology. In *Proceedings of the 32nd USENIX Conference on Security Symposium*, SEC '23, USA, 2023. USENIX Association.