

Examining the Landscape of Digital Safety and Privacy Assistance for Black Communities

Nikita Samarin
UC Berkeley

Aparna Krishnan
UT Austin

Moses Namara
Clemson University

Joanne Ma
UC Berkeley

Elissa M. Redmiles
Max Planck Institute for Software Systems

Abstract

Recent events have placed a renewed focus on the issue of racial justice in the United States and other countries. One dimension of this issue that has received considerable attention is the security and privacy threats and vulnerabilities faced by the communities of color.

Our study focuses on community-level advocates who organize workshops, clinics, and other initiatives that inform Black communities about existing digital safety and privacy threats and ways to mitigate against them. Additionally, we aim to understand the online security and privacy needs and attitudes of participants who partake in these initiatives. We hope that by understanding how advocates work in different contexts and what teaching methods are effective, we can help other digital safety experts and activists become advocates within their communities.

1 Introduction

After the death of George Floyd in May 2020, a series of large-scale protests against police brutality and racism took place across the cities in the United States and later in other countries [8]. The demonstrations, as well as the law enforcement response against the protesters, have underscored the security and privacy threats faced by communities of color [17].

However, these threats are anything but new. Over the years, researchers in various fields have published numerous articles, reports, and journalistic pieces discussing the disproportionate impact of digital safety and privacy threats on the communities of color, including the heightened risk

of surveillance of online [12] and real-world activities [16], online harassment [13], propaganda and disinformation [14], and biases in algorithmic decision-making [5]. These threats, which heighten existing inequalities and often result from actions by law enforcement and other state actors [18], violate the principles laid out in the United Nations Universal Declaration of Human Rights [1].

This study aims to understand the existing approaches to educating members of Black communities in the United States about their online security and privacy and assess how effective these approaches are. As a case example, we focus on community-level advocates who organize workshops, clinics, and other initiatives that inform members of Black communities about existing digital safety and privacy threats and ways to mitigate against them. Through interviews with advocates from civil society groups and grassroots movements that focus on the issues of digital safety and racial injustice, we plan to answer the following research questions:

- **RQ1:** What are the practices that advocates use to organize digital safety and privacy initiatives for members of Black communities?
- **RQ2:** What are the challenges that advocates encounter when organizing these initiatives?
- **RQ3:** How do advocates measure the success of the initiatives that they organize?
- **RQ4:** What is the efficacy of these initiatives in improving the digital safety and privacy for their intended audience, as perceived by the advocates and the participants of these initiatives?

Additionally, we aim to observe these practices *in-situ* by attending events hosted by the advocates and understand the online security and privacy needs and attitudes of participants who take part in these events. We hope that by understanding how advocates work in different contexts and what teaching methods are effective, we can help other digital safety experts and activists become advocates within their communities.

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2021.
August 8–10, 2021, Vancouver, B.C., Canada.

2 Related Work

Prior work has demonstrated variability in online security and privacy experiences and concerns based on race and ethnicity. A 2019 study by the Pew Research Center has reported that Black Americans are more likely to experience social media or email breaches than their white counterparts (20% vs. 6%) [2]. There are also differences in the perceived threat actor of security and privacy risks, with Black Americans being more likely than white Americans to believe that the government is tracking their activities online (60% vs. 43%) [2] and more than three times as likely to say they are concerned about being unfairly targeted by law enforcement (73% vs. 23%) [9]. Finally, there is a difference in the impact of security and privacy threats on members of different racial and ethnic groups. For instance, Black Americans are more likely to face discrimination by algorithmic decision-making processes, leading to a reduction in healthcare [10] or a higher risk of being misidentified by a facial recognition algorithm in a criminal investigation case [7].

We believe that the variability of these factors and the unique nature of digital safety threats translate into differences between the security and privacy assistance and education required for racial and ethnic minority groups compared to other populations. Furthermore, a recent study by Boyd et al. examining the security and privacy advice given to Black Lives Matter protesters has emphasized the need for future work to “further investigate and codify best practices for [...] community-based activist trainings” [3].

Some studies have also explored best practices for improving the digital safety of targeted individuals and groups by providing personalized assistance from trained teams of technologists and security experts. Such computer security clinics currently exist for victims of intimate partner violence [6], journalists [11], activists [15], and politically-vulnerable organizations [4]. Despite the increase in the prevalence of such research, no academic study known to us has explored the best practices for improving the security and privacy of Black communities in the United States using a participatory research design. Our work, therefore, will contribute to the academic literature on the security and privacy needs of underserved communities and serve as a step towards the reduction of racial inequality caused by the disproportionate impact of security and privacy threats.

3 Methodology

The study consists of three parts: an observational study, interviews with advocates, and interviews with participants. We will complete all parts of the study remotely to mitigate COVID-19 transmission risks.

To achieve our research goals, we will be closely collaborating with Matt Mitchell and Sarah Aoun from CryptoHarlem, a digital surveillance clinic that organizes impromptu work-

shops teaching basic cryptography tools to the predominately African American community in upper Manhattan.¹ Mitchell and Aoun will discuss their experiences leading workshops at CryptoHarlem and, through snowball sampling, introduce us to other community-level advocates and facilitate the recruitment of participants for our interviews.

3.1 Observational Study

Alongside the interviews, our research team will remotely participate in the workshops, clinics, and other initiatives hosted by advocates.² We shall adopt a “fly-on-the-wall” observation technique in order to note any relevant practices that occur during those events, such as the topic of the session, online platform used for content delivery, duration of the event, type of interactions between the audience and the facilitator, and so on. The findings from this part of the study will complement the results that we obtain from the interviews.

To ensure that we only perform observation of public behavior, we will observe events that are accessible to anyone who has a computer, Internet access, and, possibly, a social media account. Examples of such events include educational videos live-streamed on Twitch, Youtube, or Facebook available to all platform members. We will use the same criteria when watching the recordings of past events.

3.2 Interviews with Advocates

To gain a better understanding of the normative landscape of approaches used to inform members of Black communities about online security and privacy threats, we will perform an interview study with digital-safety advocates working at the community level. These interviews will also allow us to learn about the challenges that advocates face when they organize educational activities and the metrics that they use to measure the success of their efforts.

3.2.1 Subject Population

We will use the following criteria to select advocates to interview:

1. An “advocate” organizes, helps organize, or works with someone directly who organizes initiatives, including but not limited to: workshops, meetups, trainings, conferences, clinics, consultations, and other types of events and activities.
2. The organized initiative focuses at least partially on digital safety, online security, or privacy threat mitigation strategies applicable for individuals and communities.

¹<https://www.cryptoharlem.com/>

²These initiatives have been traditionally held in person but have since moved online due to the ongoing COVID-19 pandemic, providing the opportunity for us to attend these events remotely.

3. The advocates will decide themselves whether their initiative focuses on digital safety and privacy, to avoid the researchers imposing a definition onto them.
4. The target audience for the initiative should primarily include members of a Black community.
5. The initiative takes place on a regular basis, i.e., is held more than once with different participants.
6. The initiative takes place within the borders of the U.S. (if in person), or the advocate resides in the U.S. (if online).

We expect to interview at least 12 advocates, who will be initially identified by our partner organization CryptoHarlem. Mitchell and Aoun, who lead CryptoHarlem, will send prospective participants an invitation to complete a screening survey to determine their eligibility according to the criteria that we outline above. Respondents will also answer demographic questions and indicate their preferred contact information, allowing us to reach out to them directly to schedule the interview. We will compensate each advocate with \$30 once we complete the interview and ask them to invite other prospective participants.

3.2.2 Interview Guide

We will conduct semi-structured interviews lasting around 50 minutes to gain a better understanding of the normative landscape of approaches used to inform members of Black communities about online security and privacy threats. We will focus on four topics relevant to our research questions:

- **Motivation.**
 - How did you first get involved with this type of work?
 - What does ‘digital safety and privacy’ mean to you personally?
 - What motivates you to do this work on a regular basis?
- **Experiences with running the events.**
 - How do you go about organizing a typical event you run in your organization?
 - What are the most challenging aspects of this experience?
 - Which outreach strategies do you use to promote your events?
 - How many volunteers and supporting staff do you have to help you run the events?
 - Could you tell me about the funding that you require to run the events?

- **Teaching methods.**

- How do you choose the topic for a typical event you run in your organization?
- After you have selected a topic, how do you go about preparing to cover it during the event?

- **Success metrics.**

- How would you define ‘success’ in the work that you do?
- What is the overarching goal that your events are trying to achieve?
- What makes you say to yourself “that was a good event”?

3.3 Interviews with participants

Additionally, we aim to evaluate the efficacy of these educational initiatives—including workshops, meetups, consultations, and other activities—organized by advocates in leading to the adoption of secure online behaviors by members of Black communities. To this end, we will conduct interviews with participants of digital safety initiatives to understand their online security and privacy attitudes, needs, and concerns, as well as their experiences with the advocate-led initiatives. Both the interviews with community-level advocates and participants will help foster our understanding of how to address security- and privacy-related needs more effectively.

3.3.1 Subject Population

We will use the following criterion to select participants to interview:

1. A “participant” is someone who previously took part in an initiative organized by an “advocate.”

We aim to interview 3 to 5 participants per single initiative, and we expect to focus on at least three different types of initiatives. We will ask Mitchell and Aoun, as well as other advocates we interview, to help us reach out to the attendees of their events by sending an invitation to our screening survey. As before, respondents will answer demographic questions and indicate their preferred contact information, allowing us to reach out to them directly to schedule the interview. At the end of the interview, we will compensate each interviewee with \$20 for their participation in the study.

3.3.2 Interview Guide

We will conduct semi-structured interviews lasting around 30 minutes to explore the experiences of participants attending advocate-led initiatives and their perceptions and attitudes of digital safety and privacy. In particular, we will focus on the following three topics:

- **Background and finding out about events.**
 - How did you find out about the workshop in the first place?
 - What motivated you to attend the workshop?
 - Was there anything specific that you wanted to get out of attending the workshop?
 - Have you attended workshops from this organization or another one since the first workshop?
- **Experiences with participating in the events.**
 - Could you tell me about your experiences attending one of the workshops?
 - Based on your experience attending the workshop, what were the key lessons that you learned?
 - How easy or hard was it for you to understand the material taught in the workshop?
 - How helpful or unhelpful did you find the course material taught in the workshop?
 - Would you recommend this workshop to a friend or a colleague?
- **Privacy and security threats.**
 - What does ‘digital safety and privacy’ mean to you personally?
 - When you think about ways you keep yourself safe, what things come to mind?
 - What kind of threats or risks do you worry about?
 - Were there any specific concerns about your digital safety or privacy that led you to attend the workshop?
 - Are there any other concerns that you felt were not answered by attending these events?

3.4 Ethics

We will record audio from the interviews for transcription, coding, and analysis. The raw audio recordings will be securely stored and subsequently deleted as soon we finish transcribing them. We will also remove any sensitive and personally identifiable information contained in the interviews as part of the transcription process. Additionally, we will assign unique random identifiers to connect the survey responses and interview transcripts to the same participants; the survey responses, interview data, and the identifiers will be stored separately from any personally identifiable information.

Our team has done extensive human subjects research and has years of research experience in the privacy and security domain. All members of our research team have performed or will perform the Responsible Research and Social & Behavioral Research CITI Program training, or equivalent. The

study is currently undergoing the Institutional Review Board (IRB) review process at the University of California, Berkeley (under the protocol ID: 2021-02-14070).

Acknowledgments

We acknowledge the financial support of the Center for Technology, Society & Policy (CTSP) and the Center for Long-Term Cybersecurity (CLTC) at the University of California, Berkeley. Additionally, we would like to thank Matt Mitchell, Sarah Aoun, and Sarah Chasins for their assistance with this project.

References

- [1] United Nations. General Assembly. Universal declaration of human rights. 302(2):14–25, 1948.
- [2] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. Americans and privacy: Concerned, confused and feeling lack of control over their personal information. *Pew Research Center*, 2019. Retrieved June 10, 2021 from <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.
- [3] Maia J. Boyd, Jamar L. Sullivan Jr, Marshini Chetty, and Blase Ur. Understanding the security and privacy advice given to Black Lives Matter protesters. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–18, 2021.
- [4] Sean Brooks. Defending politically vulnerable organizations online. Technical report, Center for Long-Term Cybersecurity (CLTC), 2018. Retrieved June 25, 2020 from <https://cltc.berkeley.edu/defendingpvos/>.
- [5] Patrick Grother, Mei Ngan, and Kayee Hanaoka. *Face Recognition Vendor Test (FVRT): Part 3, Demographic Effects*. National Institute of Standards and Technology, 2019.
- [6] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. Clinical computer security for victims of intimate partner violence. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 105–122, 2019.
- [7] Brendan F. Klare, Mark J. Burge, Joshua C. Klontz, Richard W. Vorder Bruegge, and Anil K. Jain. Face recognition performance: Role of demographic information. *IEEE Transactions on Information Forensics and Security*, 7(6):1789–1801, 2012.

- [8] Hedwig Lee, Michael Esposito, Frank Edwards, Yung Chun, and Michal Grinstein-Weiss. The demographics of racial inequality in the United States. *The Brookings Institution*, 2020. Retrieved June 10, 2021 from <https://www.brookings.edu/blog/up-front/2020/07/27/the-demographics-of-racial-inequality-in-the-united-states/>.
- [9] Mary Madden. Privacy, security, and digital inequality: How technology experiences and resources vary by socioeconomic status, race, and ethnicity. *Data & Society*, Sep, 2017.
- [10] Ziad Obermeyer, Brian Powers, Christine Vogeli, and Sendhil Mullainathan. Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, 366(6464):447–453, 2019.
- [11] Shazdeh Omari. CPJ annual report 2020. *Committee to Protect Journalists*, 2020. Retrieved June 10, 2021 from <https://cpj.org/about/annual-report/>.
- [12] Desmond Upton Patton, Douglas-Wade Brunton, Andrea Dixon, Reuben Jonathan Miller, Patrick Leonard, and Rose Hackman. Stop and frisk online: Theorizing everyday racism in digital policing in the use of social media for identification of criminal conduct and associations. *Social Media+ Society*, 3(3):2056305117733344, 2017.
- [13] Kevin Rector. 911 caller in ‘swatting’ incident at BLM leader’s home said he was sending ‘message’. *Los Angeles Times*, 2020. Retrieved June 10, 2021 from <https://www.latimes.com/california/story/2020-08-13/911-caller-in-swatting-incident-at-blm-leaders-home-said-he-was-sending-a-message>.
- [14] Kevin Roose. No, a Black Lives Matter co-founder didn’t partner with a pro-communist Chinese group. *The New York Times*, 2020. Retrieved June 10, 2021 from <https://www.nytimes.com/2020/09/18/technology/no-a-black-lives-matter-co-founder-didnt-partner-with-a-pro-communist-chinese-group.html>.
- [15] John Scott-Railton. Security for the high-risk user: separate and unequal. *IEEE Security & Privacy*, 14(2):79–87, 2016.
- [16] Anjuli R. K. Shere and Jason Nurse. Police surveillance of Black Lives Matter shows the danger technology poses to democracy. *The Conversation*, 2020. Retrieved June 10, 2021 from <https://theconversation.com/police-surveillance-of-black-lives-matter-shows-the-danger-technology-poses-to-democracy-142194>.
- [17] Camille Stewart. Systemic racism is a cybersecurity threat. *The Council on Foreign Relations (CFR)*, 2020. Retrieved June 10, 2021 from <https://www.cfr.org/blog/systemic-racism-cybersecurity-threat>.
- [18] Ronald Weitzer and Steven A. Tuch. *Race and policing in America: Conflict and reform*. Cambridge University Press, 2006.