Understanding the Security and Privacy Advice Given to Black Lives Matter Protesters

Maia J. Boyd
University of Chicago
mboyd6@uchicago.edu

Jamar L. Sullivan Jr.
University of Chicago
jlsullivan2@uchicago.edu

Marshini Chetty
University of Chicago
marshini@uchicago.edu

Blase Ur
University of Chicago
blase@uchicago.edu

ABSTRACT

In 2020, there were widespread Black Lives Matter (BLM) protests in the U.S. Because many attendees were novice protesters, organizations distributed guides for staying safe at a protest, often including security and privacy advice. To understand what advice novice protesters are given, we collected 41 safety guides distributed during BLM protests in spring 2020. We identified 13 classes of digital security and privacy advice in these guides. To understand whether this advice influences protesters, we surveyed 167 BLM protesters. Respondents reported an array of security and privacy concerns, and their concerns were magnified when considering fellow protesters. While most respondents reported being aware of, and following, certain advice (e.g., choosing a strong phone passcode), many were unaware of key advice like using end-to-end encrypted messengers and disabling biometric phone unlocking. Our results can guide future advice and technologies to help novice protesters protect their security and privacy.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**.

KEYWORDS

BlackLivesMatter, Activism, Security, Black Lives Matter, BLM, Security Advice, Privacy

ACM Reference Format:
Maia J. Boyd, Jamar L. Sullivan Jr., Marshini Chetty, and Blase Ur. 2021. Understanding the Security and Privacy Advice Given to Black Lives Matter Protesters. In *CHI Conference on Human Factors in Computing Systems (CHI '21), May 8–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/3411764.3445061

1 INTRODUCTION

In early 2020, a series of high-profile cases of police brutality against Black individuals received widespread media attention. These cases included the fatal shootings of Ahmed Arbery in February and Breonna Taylor in March, as well as the killing of George Floyd in May. These events led to widespread protests in the US and internationally. An estimated 15–26 million Americans participated in these protests for the Black Lives Matter (**BLM**) movement to spur change against racial injustice. In turn, these protesters faced privacy and security threats from police and others attempting to surveil or harm the movement [41, 82, 86, 91]. Because many attendees of these protests were novice protesters, numerous organizations distributed **safety guides**, or succinct sets of advice for staying safe at a protest. These guides, such as those shown in Figure 1, often included digital security and privacy advice. Although there have been studies of how users follow security advice in general contexts [28, 39, 63, 65, 67, 68], the degree to which activists are informed about, and take advantage of, privacy and security advice remains an open question. Moreover, most HCI research on the BLM movement has focused on discourse online [2, 59, 76, 78, 81], rather than the role of technology in demonstrations and protests.

Towards helping activists stay safe at in-person protests, we answer two research questions within the context of the BLM movement.[1] First, we wanted to understand the spectrum of digital security and privacy advice novice BLM protesters are given in widely available safety guides. Second, we wanted to examine whether this advice is understood and used by novice BLM protesters. To answer these questions, we first collected 41 safety guides distributed on social media and the web during the spring 2020 BLM protests, performing content analysis on those guides. To understand whether this advice reaches and influences protesters, we then conducted an online survey of 167 BLM protesters, primarily novice protesters. The survey covered protesters' security and privacy concerns, knowledge of tools and strategies, and actions.

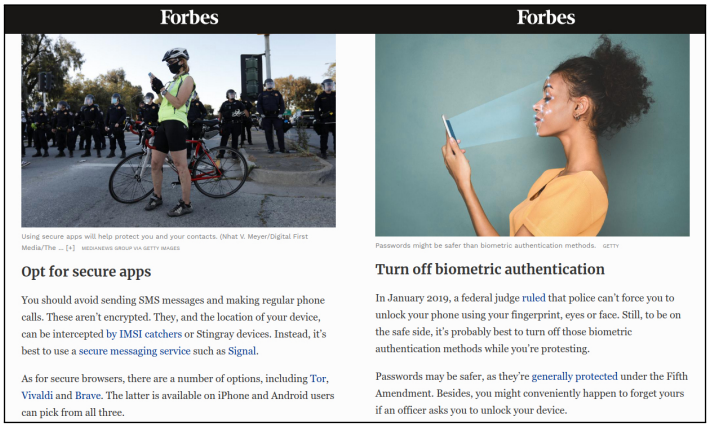
We identified 13 key classes of digital security and privacy advice given to novice protesters. The most common advice included disabling phones' transmission features (e.g., putting them in airplane mode), communicating via an end-to-end encrypted (**E2EE**) app, and disabling biometric unlocking on phones. Guides varied widely, though, in the amount and type of advice they listed, with a few guides recommending the use of VPNs, the Tor browser, and features restricting phone usage to a single app. In our survey, novice BLM activists reported an array of security and privacy concerns about attending in-person protests, and they were particularly concerned about the safety of fellow protesters. The advice most familiar to protesters – using strong passcodes on phones and

CHI '21, May 8–13, 2021, Yokohama, Japan

ACM ISBN 978-1-4503-8096-6/21/05.
https://doi.org/10.1145/3411764.3445061

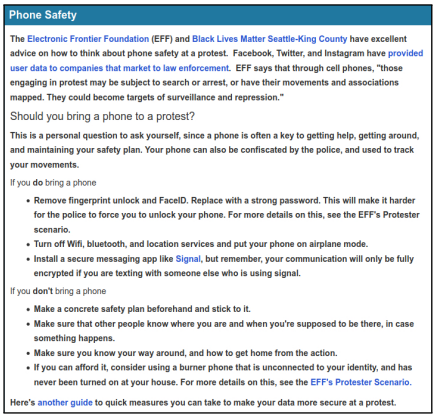
[1] Our research questions were informed in part by 20 interviews we conducted in fall 2019 and winter 2020 with BLM activists who help organize events in the movement. These interviews are outside the scope of this paper.

(a) The first and fourth images of a ten-image safety guide posted on Instagram [42], reformatted to be side-by-side.



(b) Two of the eleven privacy tips in a longer guide featured on Forbes [36], reformatted to be side-by-side.

(c) Infographic distributed on Twitter [80].



(d) From Seattle Central College [8].

(e) From BLM Belfast's guide [7].

Figure 1: Excerpts from safety guides for novice protesters distributed during BLM protests in June 2020.

being cautious about social media usage – conspicuously also applies outside of protests. Protest-specific recommendations widely reported in safety guides, including using E2EE apps instead of texting and disabling biometric phone unlocking, were not widely followed, nor fully understood. We also unpack how knowledge and usage of this advice correlated with respondents' demographics and experiences. We discuss our results' implications for the design of protest safety guides and better supporting protesters' security and privacy through community-based interventions.

2 BACKGROUND AND RELATED WORK

In this section, we introduce the BLM movement and present prior work on digital activism and advice about security and privacy.

The Black Lives Matter Movement. In 2013, after George Zimmerman was acquitted of the murder of Trayvon Martin, the Black Lives Matter (BLM) movement began with the creation of the #BlackLivesMatter hashtag on Twitter by activists Alicia Garza, Patrisse Cullors, and Opal Tometi [5, 14]. BLM is a decentralized political and social movement that focuses on minimizing police brutality against Black people and improving the lives of Black people more broadly. BLM uses social media considerably and faces the substantial challenges that come with it [89]. Over time, the movement has evolved to have a web presence and numerous chapters in the USA and Canada [6]. The BLM movement has had major increases in activity around times when very public cases of police brutality have emerged. For instance, the deaths of Michael Brown and Eric Garner in 2014 led to protests in Ferguson, Missouri and far beyond [29]. In 2020, continuing cases of egregious police brutality against Black people, such as Ahmaud Arbery, Breonna Taylor, and George Floyd, sparked widespread mass protests across the United States and the world. These protests dramatically increased participation in the BLM movement to an estimated 26 million [10]. Many of these additional protesters did not necessarily identify as being part of the BLM movement, but were supportive of rallying against violence towards Black people. This also meant that many novice protesters began attending marches and events in 2020.

There have been extensive academic studies of the BLM movement. Often, these studies investigate online BLM activities and hashtag activism, that is "the creation and proliferation of online activism stamped with a hashtag" [40]. For example, in 2016 De Choudhury et al. studied 28 million BLM tweets and how they relate to events in the real world, such as protests [24]. Another study looked into hashtags that were commonly used alongside #BlackLivesMatter around the Ferguson movement in 2014 [38]. Other research,

focused on discourse related to #BlackLivesMatter on Twitter, found that the volume and content of #BlackLivesMatter tweets spiked after major news events [1]. For instance, of the 1.3 million tweets containing the hashtag in 2018, the majority were from July 2016 when there was another series of cases of police brutality against Black people. Most recently, Stewart et al. [76] examined how positions were framed and contested through #BlackLivesMatter discourse from the political left and right. In additional studies by Stewart [77] and Arif [2], the researchers showed how bad actors created fake Black Lives Matter movement personas to infiltrate the movement and spread disinformation about BLM and police shootings to influence the 2016 US elections [75]. Other studies found that purchases of deceptive Facebook ads by bad actors increased during spikes in both online and in-person BLM activities [27].

Other BLM studies [53] not only analyzed public social media accounts, but also conducted interviews with BLM groups based on engagement. Their findings were that BLM related social media accounts are characterized by a wide range of individuals. In this work, BLM organizers viewed social media as central in organizing efforts because it mobilized internal and external forces, built coalitions among and between BLM groups, and controlled the narrative of the movement. Interestingly, a recent study of BLM chapters in Chicago, New York, Los Angeles, and Washington DC, as well as other Twitter handles for BLM- and Ferguson-related tweets, found that the majority of the tweets analyzed were focused more on 'expressive communication than strategic communication aimed at mobilizing resources and negotiating directly' with people in power who are making Black people vulnerable to police brutality [79].

We also note that related studies focus on studying digital activism on social media more generally [13, 26, 50, 51, 93], but not BLM specifically [40, 89]. For instance, Rotman et al. [50] studied the outcomes of digital participation in social movements, as well as its effects. More broadly, researchers have investigated the efficacy of digital activism and its effects on traditional activism [44, 45]. Unlike these prior studies, our work does not focus on the online activities of BLM protesters or digital activism more broadly. Instead, we focus on how newcomers to the BLM movement in 2020 viewed their own security and privacy while attending in-person events and protests as part of the BLM movement.

Privacy and Security for Black Activists. In-person activism comes not just with online risks, but also physical danger. There is a long history of government surveillance of activists around the world as part of national security efforts related to political resistance or dissent [12, 32, 70]. The United States has been in the spotlight for the targeted surveillance of activists multiple times since the 1950s because of its government-sponsored counterintelligence programs. Most notably, the FBI's COINTELPRO [17] aimed to repress the Black Panther Party and Black Americans fighting against racism, such as Dr. Martin Luther King Jr. [16, 23, 55]. Although COINTELPRO was exposed and adapted in the 1970s, surveillance efforts, both domestically and abroad, expanded post-9/11 [31, 46, 47]. BLM also appeared in the FBI's IRON FIST [73] strategy in FBI documents and correspondence from 2014. IRON FIST aimed to track so-called "Black Identity Extremists" involved in the Ferguson Protests on public venues like social media. It also focused on infiltrating BLM groups offline and online [43].

Government surveillance continues to affect the way activists organize and engage [20, 48]. Even companies can surveil activists online [83]. Counter-surveillance practices have evolved alongside technological advances. For a while, counter-surveillance practices focused on acts like disabling and avoiding surveillance cameras [52], but newer practices are more complex. With the rise of video activism, cameras have come to play a key role in activist efforts to document and share information [35, 90]. For example, the peaks of activity in BLM protests corresponded with the viral spread of videos displaying brutality against Black lives by authorities or vigilantes. Videos have also been used to document protest activities, most recently seen in documenting protests surrounding the deaths of Ahmaud Arbery, Breonna Taylor, and George Floyd. Because protesters often cannot avoid cameras, activists have taken other measures, including blurring out the faces of participants in actions [54] to protect protesters' identities without diminishing the efforts of these contemporary movements.

Other studies have shown that social media has been used to surveil and target BLM activists [49] and how the Department of Homeland Security actively monitored BLM hashtags on Twitter during protests, including surveilling high-profile BLM activists like DeRay McKesson. A growing number of studies examine public attitudes to government surveillance [25, 69, 84], but they do not focus specifically on the BLM movement or in-person protests.

Security and Privacy Advice. While we are the first (to our knowledge) to study the security and privacy advice given to novice protesters, especially within the BLM movement, researchers have studied how broader types of security and privacy advice propagate and influence user behavior (or not). In a series of studies, Redmiles et al. found that the trustworthiness of an advice source has a major impact on whether a user heeds security advice [65]. They further pointed out a digital divide in which users of lower skill levels and socioeconomic status have lower-quality advice sources [63]. While most security advice on the web is at least somewhat comprehensible and actionable, it is difficult to prioritize [67]. That said, the readability of advice remains a concern [66].

Researchers have highlighted the great amount and variety of security advice that users encounter [68], leading others to conclude that the rejection of security advice may be rational in some cases [34]. A study by Ion et al. [39] and a replication of the protocol by Busse et al. [11] noted a disconnect between how security experts and non-experts prioritize security advice. Helping to explain non-experts' opinions, Fagan and Khan found that gaps in perception can contribute to the rejection of security advice [28].

For general types of security advice, the source and delivery of advice have also been studied. For example, Nicholson et al. examined how older adults seek security information [56], while Das et al. examined the portrayal of security and privacy in news media [22]. Other research has focused on the dissemination of security knowledge and advice in the workplace [3, 4, 21, 30], including studies of how best to provide security training [71, 88]. Some researchers have also studied how the folk models of security people hold, as well as informal security stories from family and friends, affect which expert security and privacy advice users follow [62, 87]. Our work contributes further insights about how a specific type of advice, that for novice protesters, can be improved to help activists.

3 ANALYSIS OF SAFETY GUIDES

We conducted a search for safety guides for novice activists attending BLM protests, specifically guides that were widely distributed in 2020. We set out to determine which safety guides appeared in searches most frequently and what safety advice is most commonly present among these guides. These pieces of advice reflect safety and security concerns BLM activists may have, and they provide a series of steps activists can take to address these concerns. Our data collection and analysis techniques were informed by, and similar to, Pierce et al.'s study of public-facing toolkits for cybersecurity advice to help users achieve security online [60]. We use the term "safety guide" to refer to an article, picture, or text that includes advice, tips, or guidelines for protesters that address common or prevalent concerns surrounding protests. Each guide typically included a bulleted list of safety tips or a set of subheadings in which each subheading discussed a class of advice. Example guides are shown in Figure 1. We did not set a length requirement for the guides. Specifically, we collected all guides created for protesters and closely analyzed those with digital privacy and security advice.

3.1 Collection Methodology

We collected safety guides using search terms on Twitter and Google. We searched on Twitter because it remains one of the main social media platforms for BLM. We used Google because it is the most widely used search engine.

On Twitter and Google, we used the same combination of keywords for our searches: *[BLM, Black Lives Matter] [Protest] [Safety, Security, Privacy] [Guide, Tips, Advice, Recommendations, Suggestions]*. We used either "BLM" or "Black Lives Matter" first because we were searching for guides created specifically for BLM protesters. We used only "protest" as the second keyword because other synonyms (e.g., "marches," "rally") produced similar results. Example searches using the keyword combinations included "BLM Protest Security Guide" and "BLM Protest Privacy Suggestions." This resulted in a total of 30 keyword searches on each website. We only collected articles or tweets published in May–June 2020.

Twitter searches: On Twitter, we examined the first 20 tweets from each search for mentions of, and links to, safety guides. We did so because most searches resulted in fewer than 20 tweets. After collecting all of the tweets, we followed the links in the tweets and downloaded the guides mentioned. Then, we used the aforementioned criteria to determine if the article was a safety guide. This process resulted in 39 safety guides in total from Twitter. Of these guides, 15 were a flyer or picture, while 24 were written prose. We then separated the guides into two categories: guides that mentioned digital security or privacy, and guides that did not. This process resulted in 10 guides from Twitter that included digital security or privacy advice. Among these, four were flyers or images.

Google searches: We followed a similar data-collection strategy on Google. For each keyword search, we examined the first two pages of search results for mentions of, and links to, safety guides for protesters. We only examined the first 20 search results for each keyword search because very few safety guides typically appeared after the second page of search results. For each search result that appeared to link to a safety guide, we followed the link and downloaded the guide. After collecting 20 artifacts in this manner for each search, we used the aforementioned criteria to filter for safety guides. In total, we collected 52 safety guides from Google. This resulted in 31 guides from Google that included digital security or privacy advice, including one infographic.

Note that we also investigated collecting guides on Facebook and Instagram. We performed searches using the same combination of keywords on Facebook generally, as well as on BLM chapters' Facebook pages. These attempts resulted in only 1–2 guides per search. On Instagram, it is not possible to perform global text searches; instead, one can only search for hashtags or accounts. Thus, we could not replicate our methods on Instagram. Since our searches could not follow the same systematic approach or did not yield a substantial number of additional guides, we did not include guides from these social media platforms in our analyses.

Overall, we collected 91 safety guides from Twitter (39) and Google (52). Three guides came up in both our Twitter and Google searches, leaving 88 unique guides. Of the 88 unique guides, 41 mentioned digital privacy and security (13 from Twitter and 31 from Google, again double-counting three guides). These 41 guides are our final dataset. We refer to the guides in our final dataset with the prefix "G-" (short for "guide") followed by an identifying number (1–41). The URL for each guide, as well as an archive of copies of these guides, is available in our online supplementary materials [9]. For each guide, we documented the date of the guide's publication, the guide's URL, the number of times the guide appeared in different keyword searches, and the main topics that the guide mentioned. For guides linked from Twitter, we also documented the number of retweets, comments, and likes for the tweet linking to the guide.

3.2 Analysis Methodology

Our goal in analyzing the safety guides was to create a taxonomy of the types of security and privacy advice they contained. We particularly aimed to capture the nuances and quirks of what they advised, as well as how they justified this advice. Thus, we used an affinity diagramming process [33, 37]. Due to the COVID-19 pandemic, this process was performed virtually using collaborative spreadsheets and video conferencing software.

After collecting all unique safety guides, one member of the research team tagged all text from the guides that pertained to computer security or privacy. After extracting (or transcribing) that text, that researcher placed the text in initial clusters based on the device or action referenced (e.g., phone unlocking, social media). At this point, multiple members of the research team read the full set of quoted advice in each cluster and discussed them as a group. Two members of the group then began the affinity diagramming process, collaboratively and iteratively sub-dividing and combining clusters so that each cluster represented highly similar advice. To capture subtle differences in advice across guides, we permitted clusters to be hierarchical. We permitted a single quote to appear in multiple clusters.

The majority of the guides appeared to have been created by companies, rather than individuals. Of the 41 guides, 21 guides were generated by media or news companies, six by advocacy organizations, three by community organizations, and two by technology companies. Only seven guides were generated by individuals through Twitter posts, while two were created and published by

Table 1: This table (continued in Table 2) presents our clustering of the security and privacy advice presented in the 41 unique safety guides we collected. There are 13 main clusters of advice. Some clusters are hierarchical, and sub-categories of advice in this hierarchy are identified with an indentation and arrow (↪). As detailed in Section 3.2, we distinguish between advice that presents high-level recommendations (*what*), specific recommendations (*detail*), and rationale (*why*), classifying each piece of advice within a cluster as one of these three classes. For brevity, the identifiers for the guides omit the leading "G."

Advice Related to Phone Confiscation	#	Guides
Disable Biometrics	28	2–8,10–13,16,17, 20–23,25,27–31,37–41
What: Disable biometric unlocking for phones	27	2–8,11–13,16,17, 20–23,25,27–31,37–41
↪ Mentions biometrics	8	2,8,17,20,22,25,27,29
↪ Mentions fingerprint unlock	24	2–5,7,11–13,16, 20–23,25,27–31,37–41
↪ Mentions face unlock	23	2–5,7,11–13,16, 20–23,25,27–31,38–41
Detail: Step-by-step instructions	1	5
Why: Biometrics make it easier to get into phones	4	3,7,29,40
Why: In case you are coerced to unlock	3	3,25,29
Why: In case you are arrested	2	7,25
Why: In case you are approached by the police	1	13
Why: Biometrics are not legally protected	3	3,6,38
↪ Not covered by 5th Amendment	2	6,38
Strong Passcode	20	1–3,5,6,8,10–12,16, 20–23,25,27,28,33, 40,41
What: Use a strong passcode/password	5	11,16,25,27,41
What: Use a passcode not easily guessed	2	5,40
What: Use a passcode instead of biometrics	12	1,2,10,11,20–23,27,28,40,41
↪ Mentions biometrics	4	2,20,22,27
↪ Mentions face unlock	11	2,10,11,20–23,27,28,40,41
↪ Mentions fingerprint unlock	12	1,2,10,11,20–23,27,28,40,41
What: Doesn't explicitly say to disable biometrics	1	6
Detail: Use 6 digits/characters	4	6,22,28,40
Detail: Use mix of letters, numbers, and symbols	2	8,25
Detail: Use 9–12 digits/characters	1	25
Detail: Don't give in to attempted coercion	1	12
Why: Protect the data on your phone	4	5,16,20,40
↪ Protect the data from cops	3	5,16,40
Why: Can't legally be forced to give it up	3	3,8,25
↪ Mentions 5th Amendment	2	3,8
Encrypt Device	9	3,8,11,20,25,28,37,40,41
What: Encrypt device	9	3,8,11,20,25,28,37,40,41
↪ Mentions full-disk encryption	3	28,37,41
Detail: Step-by-step instructions for Android	4	8,11,25,40
Detail: iOS is encrypted if passcode enabled	4	8,11,25,41
Detail: Step-by-step instructions for iOS	2	8,41
Detail: Android often encrypted by default	1	25
Why: In case phone is seized by police	3	3,25,37
Why: Protect PII	2	3,37
Back Up Device	6	3,8,20,27,28,37
What: Back up device before protest	6	3,8,20,27,28,37
Detail: Remove PII after backing up device	1	3
Why: In case device is confiscated	1	3
Why: In case device is lost	1	37
Why: Can quickly erase data if arrested	1	27
Disable Notifications	2	1,3
What: Disable notifications when locked	1	1
What: Turn off notification message content	1	3
Detail: Step-by-step instructions	1	1
Single App	2	3,8
What: Use guided access on iOS	2	3,8
What: Use screen pinning on Android	2	3,8
Detail: Step-by-step instructions	1	3
Why: Safer for capturing media	2	3,8
↪ Audio recordings	1	8
↪ Photos	1	3
Why: Safer for using social media	1	3
Why: Safer for showing police something	1	3

Advice Related to Communications	#	Guides
E2EE App	27	1–3,5,6,8,9,11–14,16, 19–21,23–28,30,31, 36–38,40
What: Use E2EE messaging app	27	1–3,5,6,8,9,11–14,16, 19–21,23–28,30,31, 36–38,40
↪ Signal	26	1–3,5,6,8,9,11–14,16, 19–21,23–26,28,30, 31,36–38,40
↪ WhatsApp	3	5,9,25
↪ Wire	3	5,11,12
↪ Wickr	2	11,28
↪ Dust	1	12
↪ Keybase	1	12
↪ Telegram	1	36
What: Don't use other communication channels	8	2,5,8,13,24,26,27,37
↪ Text message/SMS	5	2,5,8,26,27
↪ Phone calls	3	2,8,27
↪ WhatsApp	2	13,7
↪ Social media	2	24,26
Detail: Use disappearing messages feature	6	1,3,5,11,25,28
Detail: Use Signal's password/PIN protection	3	1,3,13
Detail: Don't use cloud backups	2	25,40
Detail: Set photos to save to the cloud	1	36
Detail: Use call relays	1	3
Detail: Verify cryptographic fingerprints	1	25
Why: Safer than alternatives	2	3,36
Why: Has strong privacy measures	2	5,21
Why: Run by a nonprofit	2	5,21
Why: Doesn't collect message metadata	2	3,13
Why: It is secure	10	2,3,5,8,14,16,20,21,30,37
Why: Open-source	1	3
Why: Otherwise messages can be intercepted	3	8,12,26
Why: Otherwise you give away your location	1	8
Why: Avoid persistent message storage on device	8	1–3,5,11,25,28,38
VPN	4	3,8,12,20
What: Use a VPN	4	3,8,12,20
↪ Even when not at a protest	2	3,8
↪ A non-US/non-European VPN	1	3
↪ RiseupVPN	1	12
↪ NordVPN	1	12
Detail: Points to external instruction guide	2	3,8
Why: Encrypts all data	2	3,8
Why: Privacy	1	12
Secure Browser	3	3,8,12
What: Use a secure web browser	3	3,8,12
↪ Tor	2	3,8
↪ Brave	2	3,8
↪ Vivaldi	2	3,8
↪ Firefox	1	12
↪ Safari	1	3
↪ Not Chrome	1	3
Detail: Install ad- & tracker-blockers	1	12
Detail: Use DuckDuckGo	1	12
Detail: Don't use Google search	1	12

Table 2: This table is a continuation of Table 1, presenting the remaining clusters of security and privacy advice in the 41 safety guides we collected.

Advice About Phone Networks	#	Guides
Disable Transmissions	31	1–6,8,11–17,20,21, 23–25,27–29,31, 33–35,37–41
What: Use airplane mode	19	1,3–5,8,12–14,16,17, 23,24,27–29,37,39, 40,41
What: Turn off phone	8	2,3,5,11,13,14,24,31
Detail: Turn off location	20	1,5,6,8,10,15–17,20, 21,23–25,27,29,31, 33,34,38,40
↪ For apps	4	10,21,25,29
↪ Turn off GPS	2	17,34
Detail: Turn off Bluetooth	7	3,5,16,17,24,29,40
Detail: Turn off cellular data	7	1,3,4,24,33,35,39
Detail: Turn off WiFi	8	3,5,16,17,23,24,29,40
Detail: Remove phone battery	1	12
Detail: Put phone in Faraday bag	1	12
Detail: Turn off iOS Significant Locations	1	2
Detail: Check features in airplane mode	3	3,5,29
Detail: Airplane mode is imperfect	2	5,29
Why: Protection	7	11,13,14,27,29,37,40
↪ From tracking	4	13,27,37,40
↪ From surveillance	1	11
↪ From snooping	1	14
↪ From data being monitored	1	29
Why: Stop communicating with cell towers	5	3,5,8,11,37
Why: Avoid stingrays	4	3,8,11,14
Why: Protect location/whereabouts	7	2,15,24,25,29,37,41
↪ Protect past locations	2	15,24
↪ Protect home/work locations	1	2
Why: To save cell data allocation	1	1
Why: To save battery life	1	1
No Phone	21	2,3,5,6,8,9,11–17,20, 25,27,31,34,37,38,40
What: Leave phone at home	19	2,3,5,6,8,9,11–15,20, 25,27,31,34,37,38,40
What: Use a burner phone	16	2,3,5,8,9,11,15–17, 20,25,27,31,37,38,40
What: Use a secondary phone	2	2,11
What: Don't use a burner phone	1	13
What: Organizers take extra measures	1	13
What: Use traditional communication	1	25
Detail: Phone unconnected to your identity	5	8,16,17,27,37
↪ Limit where it's turned on	3	3,16,38
↪ Get prepaid credit	2	8,37
↪ Buy with a gift card	1	27
Detail: Swap SIMs	1	38
Detail: Remember, don't save, contacts	1	8
Why: Protection	12	2,5,6,8,11,13,14,25, 27,31,38,40
↪ Of privacy	6	2,6,11,27,31,40
↪ From surveillance	2	2,13
↪ From tracking	2	8,38
↪ From spying	1	5
↪ From snooping	1	14
↪ From linking	1	25
Why: Phone reveals your communications	2	8,27
↪ Can identify organizers	1	27
Why: Protect location/movement	3	3,8,27
↪ Where you live/work	1	3
↪ Past protest attendance	1	3
Why: Protect the data stored on the device	3	3,37,40
Why: Burner phones increase surveillance	1	13
Why: For anonymity	1	11
Why: Shield from stingrays	1	14

Advice About Info/Photo Sharing	#	Guides
Avoid Identifiers	21	3,6,8,10–13,18–22,24, 25,27,28,30–32,38,41
What: Avoid identifiable people	20	3,6,8,10–12,18–22,24, 25,27,28,30–32,38,41
↪ Faces	14	8,10,12,18,19,22,25,27, 28,30–32,38,41
↪ Distinguishing features	6	3,8,10,18,21,32
↪ Tattoos	2	G8,G10
What: Avoid identifiable locations	6	3,8,10,13,25,27
↪ Street signs	3	3,25,27
↪ Business names	1	25
↪ Landmarks	1	3
What: Avoid potentially illegal activity	1	21
Detail: Blur identifiable parts	12	3,10,18–21,24,27,28, 31,38,41
Detail: Use software	7	8,10,18,19,25,27,28,38
↪ Image Scrubber	2	10,25
↪ Signal	1	28
Detail: Remove metadata	9	3,8,10,12,13,21,24,31,41
↪ Screenshot photos before sharing	5	10,13,21,31,41
Detail: Exception for people being detained	1	12
Why: Gives away location	6	3,8,12,13,25,27
↪ Based on details in photos	3	3,25,27
↪ Based on photo metadata	3	8,12,13
Why: Facilitates identifying protesters	12	3,6,8,11,12,18,20,24,25, 27,28,32
↪ For police	6	12,18,20,24,25,27
↪ For employers	1	24
↪ For opposition groups	1	18
↪ For those wishing to harm protesters	1	20
Why: For privacy	3	24,28,31
Social Media Caution	18	1,3,10–13,19–21, 23–25,27,28,30,31,33,37
What: Be cautious about the impact on others	7	1,10,11,12,23,27,30,33
What: Don't indicate your attendance	5	12,13,21,24,37
What: Don't post future plans	3	12,24,37
What: Be cautious about streaming	3	1,11,19
What: Create separate social media accounts	3	3,27,31
What: Be cautious about documenting activity	1	23
What: Don't use Facebook/Twitter	1	37
Detail: Post afterwards, not during protest	3	10,20,27
Detail: Don't link identity to accounts	2	3,27
Detail: Remove details from account	1	30
Detail: Remove metadata from uploads	1	11
Detail: Set account to private	1	G0
Detail: Untag yourself	1	G30
Why: Protect people's identities	15	1,3,11–13,19,21,23,24, 25,27,28,30,33,37
↪ From police	6	1,13,19,21,33,37
↪ From opposition groups	3	19,25,28
↪ From employer	1	25
Why: Stop police tracking protest movement	2	11,12
Why: Keep your account history private	1	3

BLM supporters. Most of the guides were organized using either bullet points or subheadings. Overall, 24 guides used only subheadings to organize the advice, while five guides used only bullet points. Five additional guides presented the advice using both subheadings and bullet points. Of the 41 guides, 22 guides mentioned why following a piece of advice was important, while 19 did not. Only 11 guides mentioned how to follow the advice. Overall, nine of the guides only mentioned the advice and did not state how to follow it or why the protester should follow it.

Following the initial iterations of this process, we recognized that aspects of the advice could be abstracted into one of three categories: *high-level recommendations* (e.g., use an E2EE messaging app), *specific recommendations* (e.g., use the Signal E2EE app and also enable the disappearing messages feature), and *rationale* (e.g., to prevent interception by police). Respectively, we term these categories **what**, **detail**, and **why**. In subsequent iterations of affinity diagramming, we tagged each cluster as one of these three categories for clarity, and we report our findings within these categories. We continued the affinity diagramming process until the two researchers participating in this process agreed that each cluster represented a cohesive idea.

3.3 Results: Classes of Advice

Through affinity diagramming, we identified 13 key classes of security and privacy advice in the 41 safety guides we collected. Within these 13 classes, we had a total of 193 clusters and sub-clusters disentangling the advice's nuances and variations. We clustered these 13 classes of advice themselves into four groups based on the type of threat they sought to mitigate. Tables 1–2 present our full clusters, which we detail in the remainder of this section.

3.3.1 ***Advice Related to Phone Confiscation.*** Six classes of advice aimed to protect against phone confiscation:

Disable Biometrics (28 guides). Some of the most common advice, given by 28 guides, was to disable biometric unlocking. While 24 guides mentioned fingerprint unlocking or Touch ID and 23 guides mentioned Face ID, only eight used the term "biometrics." Only G-5 gave step-by-step instructions. Unfortunately, only six guides explained the rationale for doing so. Explanations varied from biometrics making it easier to get into a phone, that they *"could be used to force people to provide access to their phones"* (G29), and even more vague statements (G-13: *"it might be best to deactivate facial recognition or fingerprint unlocking if you're concerned about being approached by the police"*. Only two guides mentioned specifically that biometric disclosure can be compelled/coerced, the key rationale for this advice.

Strong Passcode (20 guides). Twenty guides recommended setting a strong passcode/password, with five using the exact terminology "strong" and two others using terminology about it not being "easily guessable." Notably, 12 guides specifically recommended a passcode/password instead of biometrics. Six guides gave detailed recommendations, often borrowed from password-composition policies like *"set up a password of at least six digits"* (G-22). Of the twenty guides that gave advice about passcodes/passwords, only seven explained why. Four mentioned protecting data on phones, three of which mentioned police (G-5: *"If your phone is unlocked, an officer might access your contacts, photos you've taken, things you've posted on social media, and other information"*). Three of the guides noted that *"cops cannot legally force you to give up your passcode"* (G25), with two specifically mentioning the Fifth Amendment.

Encrypt Device (9 guides). Nine guides suggested protesters encrypt their device/phone, with three recommending full-disk encryption. Five guides gave more detailed instructions, including four that gave instructions for manually encrypting Android devices. Four noted that iOS devices are encrypted by default if a passcode is set, while G-25 mentioned that *"many Androids are also encrypted by default."* Three of the nine guides justified the advice.

Back Up Device (6 guides). Six guides advised protesters to back their device up before attending a protest. One guide gave detailed instructions, specifically mentioning to remove personally identifiable information from the device. Three of the six guides explained this advice, though rationales varied from device confiscation to device loss to arrest.

Disable Notifications (2 guides). Two guides recommended protesters *"hide notification details when your phone is locked"* (G1), with one providing step-by-step instructions. While presumably for preventing police from seeing messages received on a locked, confiscated phone, neither guide explained its recommendation.

Single App (2 guides). Two guides recommended features that restrict phone usage to a single app: Android Guided Access and iOS Screen Pinning. Both guides provided the rationale for this recommendation, but only at an abstract level (G-3: *"It's helpful in the event that you need to show someone, including law enforcement, something on your phone"*).

3.3.2 ***Advice Related to Communications.*** Three classes of advice aimed to protect messages and web browsing:

E2EE App (27 guides). Another common type of advice was to use an end-to-end-encrypted (E2EE) messaging app, which 27 guides recommended (G-2: *"Avoid using traditional phone calls and texts if at all possible. Signal is a secure, end-to-end encrypted messaging app that offers the option to delete messages after they're sent"*). Of these guides, 26 specifically recommended Signal, three each recommended WhatsApp and Wire, two recommended Wickr, and one each recommended Dust, Keybase, and Telegram. Two guides, though, recommended against WhatsApp. Eight guides noted that an E2EE app should replace other communication methods, such as text messaging/SMS (five guides), phone calls (three guides), and social media (two guides). Nine of the 27 guides gave detailed recommendations, including Signal's disappearing messages (six guides) and password-protection features (three guides). Two guides cautioned about cloud backups. Despite the academic community's interest in E2EE authentication ceremonies for verifying others' cryptographic keys [85], only one guide recommended doing so.

While 19 of the 27 guides articulated a rationale for using an E2EE app, most were vague. The most common approach, found in ten guides, was simply to state that doing so is secure. The next most common, found in eight guides, focused on the disappearing message feature rather than the security of data in transit. Other reasons were mentioned only a few times, including that Signal is run by a nonprofit and is open-source.

VPN (4 guides). Four guides recommended that protesters configure their phone to use a Virtual Private Network (VPN), with one specifically recommending a provider outside of the US and Europe. Two guides recommended always doing so (G-3: *"In or out of a demonstration, it's always a good idea to download and set up a VPN on your phone"*). Two guides pointed to external tutorials for enabling a VPN. Three guides explained the recommendation's rationale, specifically noting encrypted connections (two guides).

Secure Browser (3 guides). Three guides recommended using a secure web browser at protests (G-8: *"As for secure browsers, there are a number of options, including Tor, Vivaldi and Brave"*). However, none articulated why protesters should do so. G-12 also recommended installing an ad-blocker and using DuckDuckGo.

3.3.3 ***Advice About Phone Networks.*** To prevent large-scale tracking, many guides recommended protesters disable their phone's communication features or, even better, not bring a phone:

Disable Transmissions (31 guides). Appearing in 31 guides, disabling transmissions from phones was the most widespread advice we observed. Overall, 18 guides recommended the use of airplane mode (G-4: *"Make sure your phone battery is fully charged and in airplane mode, with data turned off"*), while eight recommended protesters turn off their phones. In addition, guides commonly recommended turning off specific features, including location services (20 guides), WiFi (eight guides), Bluetooth (seven guides), and cellular data (seven guides). Three guides recommended verifying that individual features are actually disabled in airplane mode on a given phone. Sixteen guides articulated a rationale, though there was wide variety in the specificity. Seven guides mentioned protecting the protester's location, while four mentioned protection against tracking (G-40: *"This will make your phone leak less information that police can use to track you"*). Five guides mentioned avoiding communication with cell towers, and four mentioned stingrays. Strangely, G-1 only justified these steps as saving battery life and cellular data allocations.

No Phone (21 guides). In total, 21 guides recommended that protesters not bring their primary phone to a protest. Whereas 19 guides mentioned leaving phones at home, 16 mentioned bringing a burner phone, while two mentioned bringing a secondary phone. For example, G-31 explained, *"Using a burner phone while leaving your real device at home is the safest way to protect your identity."* That said, G-13 advised against using a burner phone by arguing that they are easier to track. Seven of the guides gave more detailed instructions, such as ensuring that a burner phone is unconnected to the protester's identity. Two guides suggested using a prepaid plan for a burner phone, while another recommended buying a burner phone with a gift card. Of the 21 guides, 14 provided a rationale. We again observed a variety of vague explanations. While 12 guides explained that this advice provides protection, the promised protection was often vague, like G-2 stating, *"To protect your privacy and prevent surveillance, the best thing you can do is leave your phone at home."* While most explanations centered on preventing tracking over communication networks, three guides mentioned that leaving a primary phone at home protects the data on the device.

3.3.4 ***Advice About Info/Photo Sharing.*** The final two classes of advice aimed to protect protesters from identification based on the information shared in photos, videos, and social media posts:

Avoid Identifiers (21 guides). Overall, 21 guides recommended protesters avoid potentially identifying information in photos and recordings shared of protests, with guides specifically mentioning to avoid people (20 guides), faces (14 guides), people's identifying features (14 guides), and locations (six guides). For example, G-8 noted, *"Try to avoid capturing details that could identify someone else or where you all are, for instance their face, tattoos and street signs."* Sixteen guides provided detailed instructions, commonly recommending that protesters blur potentially identifying features (12 guides), remove metadata (nine guides), and use software to scrub information (seven guides). Succinctly, G-3 instructed, *"Blur out other demonstrators and scrub the photos of any metadata."* Five guides recommended taking a screenshot of a photo to strip metadata. Rationales, included in 14 guides, most commonly highlighted how this information can identify protesters, including to police (six guides). It can also give away protesters' locations (six guides).

Social Media Caution (18 guides). Finally, 18 guides recommended caution when using social media in conjunction with protests, though the specific recommendations were highly variable. The most common recommendation in this class, from seven guides, involved considering the impact of social media posts on other protesters. Five guides advised against documenting attendance at a protest on social media. Three guides each recommended creating separate social media accounts, being cautious when livestreaming, and not posting about future plans. While we observed seven detailed types of advice (e.g., untagging oneself from posts), each appeared in between one and three guides. Of the 18 guides, 15 explained why. All of these guides noted that the goal was to protect the identities of protesters, with six guides specifically mentioning how social media helps police identify attendees (G-1: *"Online posts may last forever and cops can request access to them. You could accidentally put a comrade in danger"*).

4 SURVEY METHOD

To understand BLM protesters' security and privacy concerns, as well as to gauge how the security and privacy advice given in the safety guides we collected aligns with protesters' actual knowledge and actions, we conducted an online survey.

4.1 Recruitment

We recruited respondents on Prolific [61], a Mechanical Turk competitor, for a study about technology usage during BLM activism. We limited participation in this study to Prolific users who are age 18 and older, live in the United States, consider themselves supporters of BLM, and who have attended at least one BLM protest in person at any point. We were able to enforce the first two criteria using Prolific's demographic filtering mechanisms. We also used Prolific's demographic filtering mechanisms to reserve 50% of the places in our study for prospective respondents who identified as Black, while the remaining 50% of slots were open to all. Since only 7.5% of US workers on Prolific identify as Black, general recruitment would minimize Black voices and thus run contrary to

Table 3: The 13 classes of advice we studied and how they were presented to participants. We use the terminology from the left column throughout the rest of the paper.

Advice	Phrasing
Disable Biometrics	*"Disable biometric (face or fingerprint) unlocking for your phone. Use a password/passcode instead."*
Strong Passcode	*"Lock your phone with a strong password/passcode containing 6+ characters/digits."*
Encrypt Device	*"Encrypt your phone, which may require manually changing settings (Android) or setting a passcode (iOS)."*
Back Up Device	*"Back up your phone before attending a protest."*
Disable Notifications	*"Configure your phone not to show notifications when it is locked."*
Single App	*"Use the feature that limits your phone to the use of a single app."*
E2EE App	*"Use an end-to-end encrypted messaging app like Signal instead of sending text messages. Configure messages to disappear automatically."*
VPN	*"Use a VPN (Virtual Private Network)."*
Secure Browser	*"Use a security-focused web browser."*
Disable Transmissions	*"Turn off your phone completely or put it in airplane mode. Be sure to disable location services, turn off WiFi, turn off Bluetooth, and turn off cellular data."*
No Phone	*"Do not bring your primary phone to a protest. Leave it at home or use a burner phone unconnected to your identity."*
Avoid Identifiers	*"For photos and videos, avoid identifying information (people, their faces, their distinguishing features, and locations). Blur such information you capture, potentially with software. Remove photo metadata, such as by sharing screenshots of photos."*
Social Media Caution	*"Be careful about what you post on social media, especially documenting your participation in a protest. Consider how your posts might impact other protesters."*

the BLM movement. However, recruiting only Black participants would exclude the perspectives of non-Black allies in the movement. To ensure that Black voices were adequately represented in studying BLM protesters, we thus devoted half of the participant spots to respondents identifying as Black. To include non-Black BLM supporters, we left the remaining spots open for general recruitment. We compensated respondents $10 for the survey, which we advertised as taking between 45 and 60 minutes.

4.2 Survey Structure

We organized the survey into four parts. The first part asked about respondents' participation in the BLM movement. To begin, we asked respondents to describe in their own words what BLM means to them. We then asked about the number of BLM and non-BLM protests they had attended. We also asked questions on five-point Likert scales about the extent to which they considered themselves a participant and an organizer in the BLM movement. We then asked eight specific questions, again on Likert scales, about their participation in BLM online and in person (e.g., *"How often do you support BLM online by posting about BLM on social media?"*).

The second part of the survey asked about safety concerns protesters may have. First, we inquired about the level of concern respondents had for themselves. In a matrix table, we listed 15 safety concerns and asked for responses on five-point Likert scales. The order was randomized per respondent. We included safety concerns about physical well-being, being identified, being surveilled, and having a phone or information being accessed. We selected these 15 concerns to map directly to the purposes of the 13 classes of advice we observed in the safety guides, as well as concerns BLM organizers and protesters expressed in 20 interviews we conducted in fall 2019 and winter 2020. Note that these preliminary interviews are outside the scope of this paper. To better gauge potential concerns even if they did not apply directly to a given respondent, we then asked analogous questions about these 15 concerns, but about fellow protesters rather than the respondents themselves. We used parallel wording, such as rewording *"I'm concerned about my physical location being tracked at a protest"* as *"I'm concerned about fellow protesters' physical locations being tracked at a protest."*

The third part of the survey investigated respondents' knowledge and use of the 13 classes of security and privacy advice identified in the safety guides (Section 3). Each of the 13 classes of advice was represented by a succinct statement. Because our goal was to gauge respondents' knowledge and use of the advice, a key challenge was to distill into succinct statements the essence of what different safety guides said on a given topic in different ways and at varying lengths. Using our clusters from affinity diagramming as a starting point, members of the research team constructed a short statement for each class of advice. We designed each statement to embody how the guides we analyzed most commonly presented that advice by including every sub-cluster of "what" or "detail" sub-advice mentioned in at least four safety guides, if applicable. We chose this threshold because it represents 10% of our sample of guides. For example, by this metric the "No Phone" statement mentions leaving a phone at home, using a burner phone, and being sure a burner phone is not connected to the protester's identity since each was mentioned in at least four safety guides.

Table 3 shows how we presented each class of advice. For each of the 13 statements (in randomized order), we asked if the respondent had previously seen that advice about attending a protest, if they felt they understood the purpose of that advice, and if they followed that advice when attending protests. We also asked the respondent to explain in free text what they believed to be the purpose of that advice, as well as why they did or did not follow it.

In the fourth part, we briefly asked respondents about technologies they wish they had to protect their security and privacy at protests. Finally, we asked the respondent to report their demographics, including age, gender, race/ethnicity, education, and location. Because respondents' perceptions can be influenced by their technical understanding of digital security and privacy, we also asked about their tech background and computer security expertise.

4.3 Ethics and Protection of Human Subjects

Because our survey covered topics related to both digital and physical safety, as well as topics that are politically charged, we took steps to protect our human subjects. While we had initially considered recruiting on social media, anonymously compensating respondents while mitigating potential fraud is highly challenging. Therefore, we chose to recruit on Prolific, where we could compensate respondents without collecting any identifiers other than the respondent's Prolific ID number, which researchers cannot map to a real identity. Similarly, we chose not to ask directly about any activities that were potentially illegal even though they might be interesting from a security and privacy standpoint. Furthermore, to prevent re-identification of respondents in the unlikely event of a data breach, we intentionally chose to ask some information in broader categories than we might otherwise (e.g., which of five US geographic regions the respondent lived in, rather than the state).

Because BLM is an extraordinarily meaningful movement to many of its members, we also wanted prospective respondents to understand how we would use their data so that they could make an informed decision about whether to participate. Therefore, at the beginning of the study, we provided a page preceding the consent form that described our research team, motivations, and goals (see the survey instrument in our supplementary materials [9]) in greater detail than would typically be found on a consent form. Our full protocol was approved by the UChicago IRB.

4.4 Limitations

Our study should be interpreted relative to its limitations. Many responses, including about following particular advice, is self-reported. Respondents might have given answers that do not match their actual behavior if they either misunderstood what was being asked or chose to convey a particular security posture, such as a respondent reporting behaviors they do not actually engage in because they feel that they ought to be doing so. While we refined our survey wording through a series of cognitive interviews, think-aloud-based pilot testing over video chat, and small-scale pilot testing on Prolific, it may nonetheless be imperfect. Tempering the latter concern, many of our key observations center on non-adoption of security advice, which is less susceptible to self-report biases.

We used a convenience sample recruited on Prolific, and this sample is not necessarily representative of the broader population of BLM protesters because it is unclear what the overlap is between our respondents on Prolific and BLM protesters who are not on this platform. To mitigate voluntary response bias, future studies could recruit participants in other ways, such as via Twitter, through coordination with BLM chapters, or via in-person channels. Prior work has found that using online platforms for security- and privacy-related surveys can counterintuitively be more representative of the population than census-representative panels [64], and Prolific typically produces higher quality responses than Mechanical Turk [58]. Furthermore, prospective respondents might not have trusted our research group or our motivations, therefore choosing not to participate. Finally, most of our respondents were novice protesters (see Section 5.1). While such novice protesters were our primary focus, further work is needed to better understand differences in security awareness between novice and experienced protesters.

4.5 Analysis Methods

We performed both quantitative and qualitative analyses.

4.5.1 Quantitative Analysis. Many parts of our survey involved multiple choice questions on scales (e.g., Likert scales). Because one of our key goals was to understand the degree to which participants were familiar with, understood, and followed the different classes of advice, much of our data presentation is primarily descriptive.

Some of our research sub-questions, however, necessitated statistical testing. For example, we created a series of five linear regression models to understand how numerous characteristics of respondents' demographics, involvement in BLM, and technical skills correlated with five distinct dependent variables (DVs): their concern for themselves at protests; their concern for fellow protesters; whether they had heard advice; whether they felt they understood advice; and whether they followed advice. Because we were most interested in overall concern and overall awareness of advice, we averaged a given respondent's answers across the 15 concerns and across the 13 classes of advice. Therefore, we treated each DV as continuous (hence using a linear regression) as it was the average of many ordinal responses. The independent variables (IVs) were as follows: whether or not the respondent identified as black; their geographic region; their area (urban, suburban, or rural); their gender; their age range; their education level; whether or not they had a technical background; whether or not they had expertise in computer security; the degree to which they considered themselves a participant in BLM; the degree to which they considered themselves an organizer of BLM; the number of years they had been part of BLM; and the number of BLM protests they had attended (with 5+ protests grouped as a single category). For categorical variables, we binned similar categories (e.g., age ranges) when there were few responses in a category. For each categorical IV, we used the most frequent response (e.g., not having a technical background) as the baseline category. We always report a parsimonious model developed through backward selection by AIC.

We were also interested in how respondents' concerns for fellow protesters compared to those for themselves. For each of the 15 concerns, we thus compared a respondent's concern for themselves and for fellow protesters using a paired Wilcoxon signed-rank test.

For all statistical analysis, $\alpha = .05$, though we also report (and clearly label) marginally significant results ($.05 \leq p \leq .10$). We corrected for multiple testing using the Benjamini-Hochberg method. We applied this correction across all five regression models, as well as across all 15 paired Wilcoxon signed-rank tests.

4.5.2 Qualitative Analysis. We also used qualitative methods to better understand respondents' free-text responses. In particular, for each of the 13 classes of advice, we coded the responses about what the respondent thought the purpose of the advice was and why they did (or did not) follow it. Through open and axial coding, two members of the research team collaboratively developed a codebook for each question by reading through all responses and discussing common themes they observed, in addition to those themes' connections. Because the topics mentioned in responses were frequently specific to a particular class of advice, each question necessitated its own codebook, though we reused codes across codebooks when applicable. Using these tentative codebooks, one

member of the research team coded all responses and updated the codebook as needed. A second coder used the updated codebook to independently code the data. We calculated intercoder agreement per codebook. The median Cohen's κ was 0.63 across codebooks.

5 SURVEY RESULTS

We first describe our respondents (Section 5.1) and their concerns at protests (Section 5.2). The subsequent five sections describe the degree to which respondents reported having heard, understood the purpose of, and followed particular advice. We again group the 13 classes of advice by the primary threat they attempt to mitigate. Finally, we report how responses to all three questions correlated with demographics and participation in BLM (Section 5.8).

5.1 Respondents and Their BLM Involvement

We collected responses from 200 crowdworkers on Prolific in late August and early September 2020. Despite the requirements we posted in bold as part of our recruitment text, 26 respondents reported in the survey that they had never been to a protest, so we did not analyze their data further. We additionally excluded three responses containing one-word answers to all free-response questions and four responses from two unique individuals who each took the survey twice from the same computer under different Prolific IDs. This filtering left 167 respondents in our final sample. Respondents completed the survey in an average of 44.9 minutes (median: 37.4 minutes).

Respondent Demographics. Following best practices [74], we gave respondents the option of selecting that they identify as a woman, identify as a man, or identify as non-binary. We also gave respondents the option to self-describe or decline to answer. Among our 167 respondents, 53% identify as a woman, 46% as a man, and 1% as non-binary. None chose to self-describe or decline to answer. Consistent with the ages of protesters in the BLM movement broadly [92], our sample skewed young relative to the broader US population. Respondents fell into the following age ranges: 18–24 (35%), 25–34 (47%), 35–44 (16%), 45–54 (2%), and 55–64 (1%). We binned (combined) the last three groups in statistical analyses.

We asked participants to select all races and ethnicities with which they identified from a list of six options adapted from the US Census, with the additional opportunity to either self-describe or decline to answer. All respondents chose to describe themselves using some combination of these six options, with 52% selecting only "Black or African American," 31% selecting only "White or Caucasian," 5% selecting only "Asian," 5% selecting only "Hispanic or Latinx," 1% selecting only "Native American or Alaskan Native," and the remaining 6% selecting more than one option. Ultimately, 56% of respondents identified at least in part as Black, while 44% did not. While a statistical model cannot hope to capture the intersectional complexities of race in the US [57], we use this binarization of Blackness as one (imperfect) covariate in our statistical analyses.

By virtue of our inclusion criteria, all respondents hailed from the United States. Respondents lived in various regions[2] of the country: the southeast (34%), northeast (28%), midwest (16%), west (13%), and southwest (9%). Among respondents, 53% reported living in an urban area, 42% in a suburban area, and 5% in a rural area.

Respondents varied in educational attainment: 17% had a high school education or less, 26% had completed some college coursework without receiving a degree, 37% held a two- or four-year college degree, and 20% held a graduate or professional degree. Among respondents, 75% did not have a technical background (defined as a degree or job in computer science, IT, or a related field). 81% reported that they did not have expertise in computer security.

Involvement in BLM. All respondents considered themselves part of the BLM movement to at least a small extent. Among respondents, 81% considered themselves part of the movement to at least a "moderate extent," while 45% considered themselves part of the movement to a "great extent" or "very great extent." In contrast, few respondents considered themselves organizers. Only 7% considered themselves organizers of the movement to a "great extent" or "very great extent," whereas 53% felt they were "not at all" organizers. The median participant had been part of the BLM movement for two years. While 26% of respondents reported joining the BLM movement in the years 2013–2015, another 28% reported joining the movement only in 2020. Among respondents, 98% reported "reading information about BLM or related events" online at least monthly. In fact, 47% described doing so at least daily. Respondents also reported participating in BLM at least monthly in other ways: "posting about BLM on social media" (87% of respondents), "signing petitions that are supported by the BLM movement" (87%), and "helping to distribute information about BLM events" (77%). A small fraction of respondents engaged in any of the following activities at least monthly: "donating money to the BLM movement or related causes supported by BLM" (54%), "helping to plan BLM events" (35%), and "attending BLM general meetings or events (other than protests)" (34%). In other words, respondents' involvement in BLM was primarily through online engagement and social media.

By virtue of our inclusion criteria, all respondents had attended a BLM protest in person. The median respondent had attended two BLM protests in the year 2020, one BLM protest prior to 2020, and one non-BLM protest at any point. Of the 167 respondents, 12 had been to at least 10 BLM protests, while two of them had been to over 50 BLM protests. Most respondents had been to only a few: 22% had been to one protest, 25% to two, 16% to three, and 12% to four. The final 25% of respondents had been to five or more. Overall, participants were novice protesters; 56% of respondents had attended between zero and two protests of any kind prior to 2020, while 20% of respondents had never been to any protest prior to 2020. Furthermore, many respondents' activism was focused on BLM. At the time of the survey, 38% of respondents had never attended any non-BLM protests, while 67% had attended at most two non-BLM protests. In short, while a few respondents were experienced protesters or organizers, most were novice protesters.

5.2 Concerns While Protesting

To contextualize respondents' decision to follow (or not to follow) particular security- and privacy-related advice at BLM protests, we aimed to understand their underlying concerns. To that end, we developed a list of 15 potential concerns about protests, as detailed

[2]We followed National Geographic's division of the US into five regions: https://www.nationalgeographic.org/maps/united-states-regions/

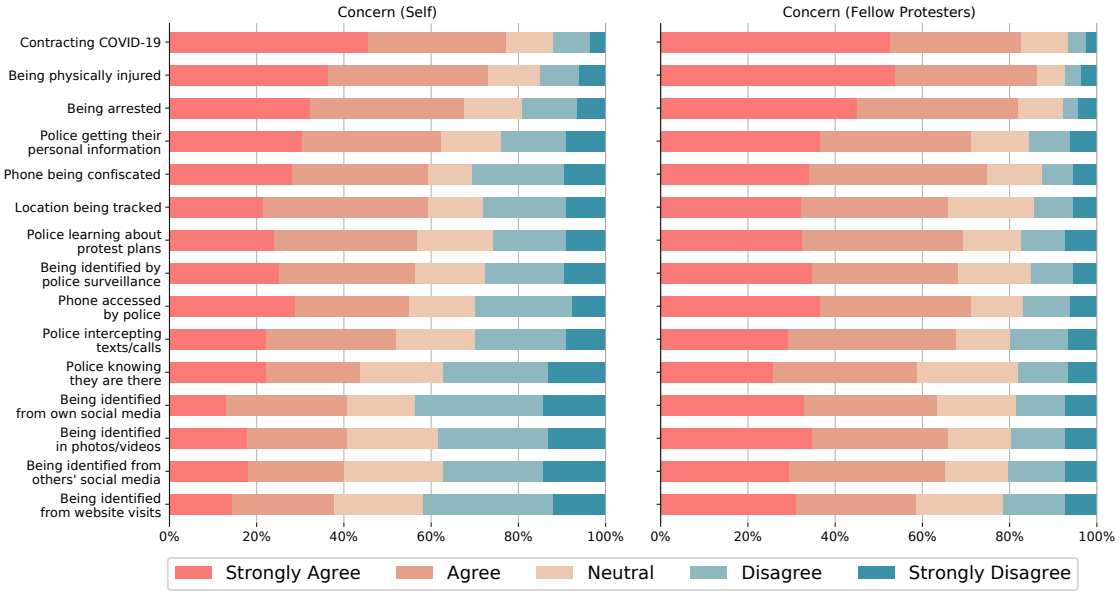


Figure 2: The distribution of respondents' level of concern about their own safety (L) and that of others (R) at BLM protests.

in Section 4.2. Most potential concerns related to security and privacy, but we also included general concerns (e.g., violence) and concerns about COVID-19 as points of comparison. Respondents first answered about these concerns for themselves, and then about fellow protesters. Responses were on a five-point Likert scale. For brevity, throughout this section we write that respondents had a concern if they answered "agree" or "strongly agree."

Concerns For Self. Figure 2 shows the distribution of concern respondents expressed about their own safety and that of fellow protesters. For themselves, the largest fraction of respondents worried about contracting COVID-19 (77%), though nearly as many worried about being injured (73%) or arrested (68%) at a protest. More than half of respondents (52%–62%) had concerns related to technology and surveillance, including that their phone would be confiscated, location tracked, messages intercepted, or phone accessed by police. A similar fraction of respondents were concerned more broadly about the police getting their personal information, identifying them via surveillance technologies, or learning about the plans for the protest. Somewhat fewer respondents were concerned about being identified based on their web browsing (38%), as well as their own (41%) or others' (40%) activity on social media.

Concerns For Fellow Protesters. The relative ranking of concerns was similar for fellow protesters, though respondents expressed greater concern for fellow protesters than for themselves. For each of the 15 potential concerns, we compared respondents' concern for themselves and fellow protesters using paired Wilcoxon signed-rank tests. Concern for fellow protesters was significantly higher than for respondents themselves in all cases (every $p < .006$). For example, whereas 59% of respondents were concerned about their phone being confiscated by police, 75% were concerned about a fellow protester's phone being confiscated.

Table 4: Our parsimonious linear regression model for respondents' concern for themselves at protests from 1 ("strongly disagree") – 5 ("strongly agree"), averaged across all 15 potential concerns. The number of protests was ordinal with bins 1, 2, 3, 4, and 5+. It was modeled quadratically.

Factor	Baseline	β	SE	t	p
(Intercept)		3.380	0.078	43.425	**<.001**
# BLM Protests Attended	(Quadratic fit)	0.429	0.169	2.546	**.032**

Table 5: Our parsimonious linear regression model for respondents' concern for fellow protesters from 1 ("strongly disagree") – 5 ("strongly agree"), averaged across all 15 potential concerns. For categorical independent variables, we indicate the baseline category.

Factor	Baseline	β	SE	t	p
(Intercept)		3.681	0.163	22.517	**<.001**
Race/Ethnicity: Non-Black	Black	0.367	0.148	2.483	**.032**
Gender: Man	Woman	-0.389	0.148	-2.636	**.032**
Gender: Non-binary	Woman	-0.400	0.672	-0.596	.552
Age Range: 18–24	25–34	0.248	0.163	1.525	.166
Age Range: 35+	25–34	-0.133	0.201	-0.661	.540
Years In BLM	(Continuous)	0.053	0.032	1.666	.146

5.3 Awareness, Knowledge, and Use of Advice

Our survey asked a series of questions about the 13 classes of advice from the safety guides. Here, we detail the degree to which respondents reported having heard each class of advice, reported understanding the purpose of that advice, and reported following that advice when attending protests. We present these results in four groups, respectively covering six classes of advice that protect protesters if their phone is confiscated (Section 5.4), three classes of advice about protecting communications (Section 5.5), two classes of advice about phone tracking (Section 5.6), and two classes of advice about sharing information and images (Section 5.7).

For brevity in writing, we report responses in bins, combining related responses on the various Likert scales. For instance, we combine answers like "a great deal" or "a moderate amount" when writing that a given fraction of participants had previously heard particular advice. Similarly, we combine answers like "strongly disagree" or "disagree" and instead write that all such participants felt they did not understand the purpose of particular advice. We only report bins at the poles of each Likert scale; we do not report on "neutral" or "not applicable" responses. In describing respondents' explanations, we report the number of participants (out of 167) whose justifications mentioned a particular theme identified in our coding process. Because these are free-response prompts, not mentioning something does not imply that a participant does not believe it. Therefore, the percentage of participants who mentioned a theme does not imply a generalizable fraction. Nonetheless, we provide these counts to give a more accurate picture of the prevalence of themes in our data. We attribute quotes using the terminology *R-#*.

5.4 Advice Related to Phone Confiscation

Six classes of advice from the safety guides would protect protesters in case their phone is confiscated. Participants widely knew about and followed common advice to lock their phone with a strong passcode, yet were less knowledgeable about (and less likely to follow) other relevant advice that appeared less commonly in safety guides. Advice about disabling biometric unlocking was common in safety guides, yet not as widely known about, nor followed.

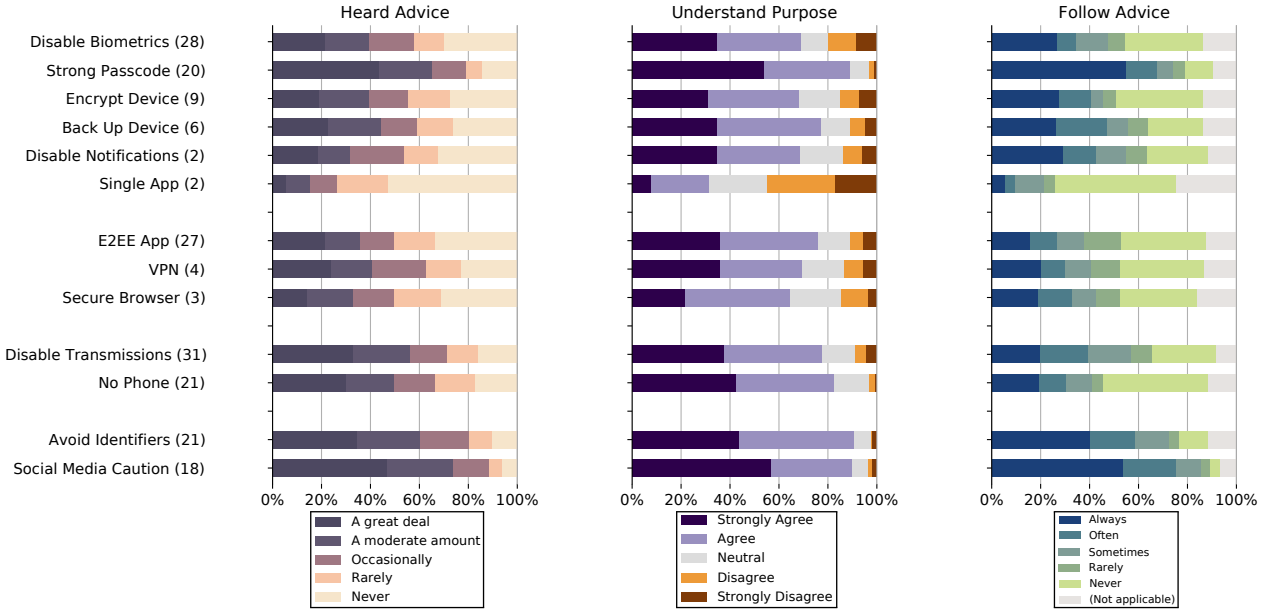
Strong Passcode. Locking phones with strong passcodes minimizes the potential for guessing attacks if they are confiscated. Overall, 65% of respondents had heard of using a strong passcode when attending protests, while 21% had not. Overall, 89% of respondents felt they understood this advice, whereas only 3% did not. In their explanations, 112 respondents correctly stated that the purpose of this advice is to prevent the police or anyone else from gaining access to a protester's phone without permission, while 31 respondents stated more generally that the purpose was to protect the information on a phone. The majority of respondents followed this advice. Their free-response explanations, though, suggested that part of the reason is that the same advice applies outside of protests. Notably, 49 respondents clarified that they always use a strong passcode whether or not they are protesting. For example, R-92 stated, *"I have followed this advice since even before I began attending protests."* More generally, 25 respondents reported following this advice to protect the information on their phone. On the other hand, 15 respondents did not use strong passwords because they did not feel it was necessary, usually citing common tropes of privacy [72] (e.g., R-130: *"I have nothing to hide"*).

Disable Biometrics. Regardless of the strength of the phone's passcode, leaving biometric unlocking enabled continues to leave a phone vulnerable because, unlike a passcode, biometrics are vulnerable to coercion. Even though disabling biometric unlocking was the second-most-common class of advice in the safety guides, only 40% of respondents had heard this advice, whereas 42% had not. Overall, 69% of respondents felt they understood the purpose of disabling biometric unlocking. Some explanations correctly identified that biometrics can be coerced, albeit in different words; 30 respondents explained that police can forcefully access a protester's phone by using their face or fingerprint without their permission, while another 27 respondents gave a similar explanation without specifically mentioning police. For example, R-145 stated, *"While police cannot force you to open the phone or divulge a passcode, they could physically force a fingerprint… to open the phone."* Whereas only 3% of respondents felt they did not understand the purpose of a strong passcode, 20% of respondents felt they did not understand the purpose of disabling biometric unlocking. Furthermore, the free-response justifications of even some respondents who felt they understood the purpose suggested that they might not. For example, eight such respondents stated that biometrics are more secure than passwords, missing that biometric unlocking typically falls back to a password [15].

Encrypt Device. Advice about encrypting devices (e.g., phones) and backing them up before protests was mentioned in a moderate number of safety guides (9 and 6, respectively), yet respondents had mixed knowledge about these practices. Among respondents, 40% had heard advice about encrypting devices they bring to protests, while 44% had heard advice about backing them up. In total, 68% felt they understood the purpose of encryption, while 77% felt they understood the purpose of back-ups. For encryption, 55 respondents wrote that the purpose was to make it harder for the police or others to gain access to phones, while 36 respondents wrote that it was to protect the data stored on phones. Similarly, 95 respondents wrote that the purpose of backing up a device is to easily retrieve important information in the future. More specific to protesting, 78 respondents mentioned the need to do so if their phone is lost or destroyed, while 68 respondents mentioned the need to do so if the phone is confiscated, including by police.

Back Up Device. Overall, 41% of respondents reported encrypting their phone, while 35% reported backing up their device before protesting. In each case, a roughly equal number reported not doing so (41% and 38%, respectively). 23 respondents reported that their phone is always encrypted even outside protests. Among those who do not encrypt their phone, 23 respondents did not think it was necessary, while 20 respondents reported that they did not do so because they do not understand the advice. Not seeing potential threats, R-100 stated, *"I don't have anything on my phone that I wouldn't be willing to show anyone including the police."* Reflecting a lack of knowledge, R-69 wrote that encrypting a phone *"seems harder- I don't know exactly how to do it, and it seems like it would take too much time to accomplish."* Regarding backing up phones, 29 respondents said they do so to avoid losing important information. Notably, 29 respondents reported routinely backing up their device whether or not they were attending a protest. In contrast, 27 respondents stated that backing up their device was not necessary, including R-81: *"I don't plan on being arrested or having my phone taken away from me."*

Disable Notifications and Single App. Among the less common suggestions were disabling notifications when a phone is locked or using features that restrict the phone to a single app. Each was found in only two safety guides. Unsurprisingly, then, only 32% of respondents had heard advice about disabling notifications, while only 16% had heard of restricting the phone to a



(a) "I have seen or heard similar advice about attending a protest."

(b) "I feel that I understand the purpose of this advice about attending a protest."

(c) "I follow this advice when attending a protest."

Figure 3: Whether respondents had (a) heard about, (b) felt they understood the purpose of, and (c) followed particular advice. The number in parentheses for each class of advice indicates how many safety guides (out of 41) mentioned that advice.

single app. Whereas 69% of respondents felt they understood the purpose of disabling notifications, only 32% felt the same about restricting the phone to a single app. The latter was, by far, the class of advice respondents least felt they understood the rationale behind. 36 respondents incorrectly stated that the purpose was to prevent location tracking.

5.5 Advice Related to Communications

To protect communications, 27 safety guides recommended that protesters use an E2EE messaging app, four recommended VPNs, and three recommended secure browsers. Nonetheless, fewer participants reported using an E2EE app than using a VPN or a secure browser, highlighting a gap between recommendations and actions.

E2EE App. Despite the wide availability and key security benefits of E2EE messaging apps like Signal, only 36% of respondents had heard to send messages on E2EE apps instead of via text messaging. Notably, 50% had not heard such advice. Nonetheless, 76% of respondents felt they understood the purpose of this advice. In particular, 44 respondents stated that the purpose was to make sure that messages between protesters were protected or secure, while 35 respondents stated that the purpose was to ensure police would be unable to read or access previous messages between protesters. Unfortunately, only 27% of respondents followed this advice; 50% did not. 61 respondents wrote that they did not use an E2EE app because they felt it was not necessary or was too drastic. Notably, 17 respondents reported that using an E2EE app is not necessary for them because they do not text during (or about) protests, while 14 reported that their messages are not important enough to use such apps. For example, R-67 stated, *"I'm not in communication with the protest organizers so my potential benefit to police is little."* In contrast, respondents that frequently used E2EE apps did so in order to protect their privacy and communications with fellow protesters. R-77 stated, *"Without access to the information shared between me and other protesters, the police would not be able to identify others involved."* While most respondents understood this recommendation, many did not.

VPN and Secure Browser. Less commonly, safety guides occasionally recommended using a VPN (4 guides) or secure web browser (3 guides). Among respondents, 41% had heard advice about using a VPN, whereas 37% had not. Similarly, 33% had heard about using a secure web browser, while 41% had not. Roughly two-thirds of respondents (69% for using a VPN, 65% for using a secure browser) felt they understood the purpose of the advice. In explaining their perceptions of the purpose of using a VPN, 73 respondents stated that it is to prevent location tracking, while 40 respondents stated that it is to protect private information like browsing history. In explaining their perceptions of the purpose of using a secure browser, 48 respondents wrote that it is to protect private information, while 36 respondents wrote that it is to stop the police or others from tracking protesters through their browsing history. Among respondents, 30% reported using a VPN, while 33% reported using a secure browser. In explaining their use of a VPN, 18 respondents aimed to prevent location tracking, such as R-44's *"to feel protected and safe from tracking devices and the police."* Notably, 13 respondents wrote that they use a VPN whether or not they are attending a protest. Respondents reported using a secure browser to stay secure (20 respondents) or to keep their browser history private (16 respondents).

5.6 Advice About Phone Networks

To prevent tracking, many guides recommend participants disable their phone's transmission features or avoid bringing a primary phone at all. Respondents were relatively familiar with both classes of advice, though observance of this advice was mixed.

Disable Transmissions. Overall, 56% of respondents had heard to disable their communication features individually or by turning on airplane mode, while 29% had not. Nonetheless, 78% felt they understood the purpose of this advice, while only 9% did not. Capturing the essence of the purpose, 121 respondents wrote that the goal is to prevent the police or others from tracking potential protesters' locations. For example, R-118 stated, *"The purpose of turning off your phone data is to keep you from being traced or tracked."* Unfortunately, while 40% of respondents followed this advice, 35% did not. Those who followed the advice did so to protect their location and identity (31 respondents) or simply to stay safe (26 respondents). For example, R-114 wrote, *"I may not completely turn my phone off, but I do happen to turn off all of my location services. This is used because I understand that I can be tracked not only during the protests, which may impact the safety of my fellow protesters, but also that I may be tracked to my home address."*

No Phone. Similarly, 50% of respondents had heard advice to avoid bringing a primary phone to protests, while 34% had not. Overwhelmingly, 83% of respondents felt they understood the purpose of doing so, while only 3% did not. Respondents' explanations of the purpose encompassed not just tracking over networks, but also the possibility of confiscation. Both of these aspects are reasons not to bring a primary phone to a protest. More precisely, 51 respondents identified the purpose as protecting private information on phones, such as information about the protest, while 49 respondents identified the purpose as protecting the identity of yourself and other protesters. For example, R-145 wrote, *"If your phone is confiscated, lost, stolen, or destroyed, it keeps your personal phone safe and in the case of a burner phone, it keeps your personal information safe if the phone gets into the wrong hands."*

Although advice to bring only a burner phone or no phone at all was relatively common in safety guides, only 31% of respondents followed this advice, whereas 47% did not. Some respondents followed this advice to stay safe (15) or to protect their privacy or identity (10). In contrast, other respondents did not follow this advice because they believe it unnecessary (31), feel that purchasing a burner phone is too expensive (20), or do not currently have a burner phone (16). For example, R-113 stated, *"I don't attend protests regularly and haven't had the money to get a burner phone."*

5.7 Advice About Info/Photo Sharing

To protect protesters, safety guides suggested taking care with potential identifiers in photos and social media posts.

Avoid Identifiers. Avoiding potential identifying information in photos or videos taken and shared of protests was among the most familiar pieces of advice; 60% of respondents had heard it, whereas only 20% had not. Similarly, 91% of respondents reported understanding the purpose of doing so, whereas only 2% did not. In their justifications, 113 respondents correctly stated that the purpose is to prevent location tracking or the identification of protesters This advice was also among the advice most widely followed, with 59% doing so and 16% not doing so. 70 respondents' reasons for doing so centered on the protection of other protesters. Of those 70, 39 respondents articulated their rationale as keeping other protesters safe from harm, while 31 articulated it as protecting other protesters' identities. R-62 wrote, *"The security and well-being of my fellow protesters is a top priority. I wouldn't ever want to put out information that could be incriminating to them. I'll always try to blur the faces of the people around me at a protest."*

Social Media Caution. Exercising caution on social media was also among the most familiar advice. Overall, 74% had heard such advice (versus 11% not) and 90% felt they understood its purpose (versus 4% not). In total, 52 respondents identified that the purpose was to protect protesters' identity and location. Additionally, 35 respondents stated that it related to keeping protesters safe, and 23 respondents specifically noted that posts on social media can be used to incriminate yourself or others. For example, R-67 wrote, *"Posts can have reprocussions [sic] either from employers, the police, or friends/family."* Respondents overwhelmingly followed this advice, 76% versus 8%. From their justifications, 38 respondents did so for safety, 29 respondents already do not post often on social media, and 25 respondents did so to protect privacy.

5.8 Regression Models of Correlations

We again built linear regression models to analyze how respondents' demographics and participation in BLM correlated with their answers about the degree to which they had heard, understood the purpose of, and followed particular advice. For each model, we averaged a respondent's answers across all 13 classes of advice, hence our choice of a linear model. Respondents were significantly more likely to report that they had heard the security and privacy advice (Table 6) if they held a degree or job related to technology ($p = .032$) or if they considered themselves a BLM organizer to a greater degree ($p = .013$). These results have the potential explanation that familiarity with IT-related topics or being involved as a BLM organizer both make it more likely that a respondent would have encountered advice about computer security or privacy.

Table 7 presents our model for understanding the purpose of advice. Respondents who more strongly identified as BLM participants were more likely to feel that they understood the advice's purpose ($p = .016$). In addition, compared to those who lived in an urban area, respondents were marginally more likely to feel that they understood the advice's purpose if they lived in a suburban area ($p = .063$). Our parsimonious model for following advice (Table 8) was similar to that for having heard advice. Respondents who held a degree or job related to technology ($p = .013$) or who considered themselves a BLM organizer to a greater degree ($p = .013$) reported following the 13 classes of advice more frequently. A potential explanation may be that both types of respondents have a clearer understanding of potential consequences.

6 DISCUSSION

We analyzed 41 safety guides, identifying 13 classes of digital security and privacy advice given to novice BLM protesters. We also conducted a survey of 167 BLM protesters to see what concerns they had for in-person events, as well as whether they had heard

Table 6: Our parsimonious linear regression model analyzing correlations between respondents' ratings for whether they had heard particular advice from 1 ("never") – 5 ("a great deal"), averaged across all 13 classes of advice, and their demographics. For categorical independent variables (IVs), we indicate the baseline category. For ordinal IVs, we indicate the fitted function.

Factor	Baseline	β	SE	t	p
(Intercept)	–	3.237	0.150	21.618	**<.001**
Gender: Man	Woman	0.246	0.139	1.773	.128
Gender: Non-binary	Woman	0.821	0.636	1.291	.238
Tech Background: Yes	No	0.539	0.217	2.490	**.032**
Security Background: Yes	No	-0.376	0.241	-1.563	.166
Consider Self BLM Organizer	(Linear fit)	0.903	0.289	3.127	**.013**

Table 7: Our parsimonious model analyzing correlations between respondents' ratings for whether they felt they understood advice's purpose from 1 ("strongly disagree") – 5 ("strongly agree"), averaged across all 13 classes of advice, and their demographics.

Factor	Baseline	β	SE	t	p
(Intercept)	–	3.845	0.071	54.030	**<.001**
Area: Suburban	Urban	0.214	0.098	2.168	.063
Area: Rural	Urban	-0.253	0.214	-1.185	.267
Tech Background: Yes	No	0.201	0.112	1.793	.128
Consider Self BLM Participant	(Quadratic fit)	0.293	0.099	2.951	**.016**

Table 8: Our parsimonious model analyzing correlations between respondents' ratings for whether they followed particular advice from 0 ("not applicable") – 5 ("always"), averaged across all 13 classes of advice, and their demographics.

Factor	Baseline	β	SE	t	p
(Intercept)	–	2.947	0.147	20.107	**<.001**
Tech Background: Yes	No	0.609	0.183	3.322	**.013**
Consider Self BLM Organizer	(Linear fit)	0.991	0.318	3.115	**.013**

of, understood the purpose of, and followed the types of advice presented in these safety guides.

6.1 Implications For Safety Guides

In our analysis of the safety guides, two of the most common pieces of advice were to disable biometric unlocking of phones and to use an E2EE messaging app instead of text messages. However, in our survey, these very same pieces of advice were less known to our respondents, less understood overall in terms of how they protect digital security and privacy, and even more rarely followed. In contrast, other common pieces of advice, such as having a strong passcode, avoiding identifying information in photos, and avoiding social media posts, were more commonly known, understood, and followed. This result suggests several disconnects.

6.1.1 Prioritizing Advice For The Target Audience. First, the safety guides themselves are often dense with tips. It may be easier for protesters to have a prioritized list of advice. For instance, a one-time protester may only be interested in the top three suggestions for keeping safe. Prioritized advice lists might be more effective if they could list what suggestions offer the most protection for little effort, or based on time to prepare, or even how involved the person is in the movement. For instance, some guides offered specialized advice, such as using a VPN, Brave browser, or Tor. These steps seem targeted at long-term protesters and activists. It would help novice protesters to better understand which of the many pieces of advice are more pertinent to them. In addition, in our study, only two guides appeared to have been created and distributed by BLM supporters. The majority of the guides were made by news organizations. This finding suggests that there is room to expand on the current offerings with guides specific to BLM or other activist causes. Future qualitative studies could examine the security and privacy needs of novice in-person protesters in more depth so that guides and other supportive services can be tailored to user needs.

6.1.2 Improving Information Presentation. Second, patterns in our survey responses suggest that when the purpose of particular advice was poorly understood, it was less followed overall. In contrast, if respondents were aware of clear steps for following the advice, they were more likely to follow it. Lastly, if respondents felt the advice was "necessary," then they were more likely to follow it. For instance, for a one-time protester, a burner phone was considered unnecessary. In the guides themselves, these issues around the ease of following the advice and what the advice affords could be addressed through improving the presentation of the advice.

Instead of only providing a suggestion, the "why" and "how" of the suggestion are equally important aspects of security advice. Unfortunately, only about half of the guides we studied provided this "why," and only about a quarter provided the "how." That is, our respondents needed to know what protections are afforded by the suggestion. For unfamiliar advice, they also needed detailed steps on how to accomplish the suggestion, which would lower the barrier to adopting that advice during protests.

Key open questions include what forms of presentation are most effective for helping protesters understand and follow advice. For instance, is an infographic more effective than a guide with tips? Are there other ways to package up advice in easily consumable forms for different audiences? Are bulleted lists more effective than using subheadings? Where should the "how" and "why" be included? Future work also needs to understand how to delineate the target audience and how to distribute the advice widely to activists or other supporters of the movement. Additionally, although this did not come up in our study, another open question is how to ensure that the credibility of the advice is clear. In our ongoing work to improve the understanding of why particular advice should be followed, we are currently developing a mobile app that will show protesters what data can be gathered from their phones if they do not enable certain protections. We plan to use this app to gather additional data on how best to help in-person novice protesters maintain their security and privacy. This work is inspired by the WiFi privacy ticker [18], in which researchers showed users how insecure WiFi is by showing them the data that is sent over the wireless connection in plaintext.

6.2 Implications for Community Engagement

It was clear from our respondents' encounters with advice that keeping activists safe also means tackling issues around the distribution of information. Often, respondents holding technology-oriented jobs had heard various pieces of advice, particularly more

obscure suggestions like restricting a phone to a single app. To help protesters of all technology backgrounds keep safe, the community may need alternative channels to distribute advice to activists. Certainly, this could be done online, but we suggest an alternative path to distribute safety advice that leverages the community aspect of BLM and other activist movements. We suggest that helping protesters and activists learn about safety advice through in-person trainings, meet-ups, or events could be a vessel both to get more people to engage and to ensure that they can do so with minimal risk to themselves and their fellow protesters. For instance, another barrier to using end-to-end encryption is the process of installing an app like Signal, as well as ascertaining that other members of one's communication network are on the same platform. "Installation parties" for key apps like Signal could help get everyone to a point where they can safely engage with others in the movement without having to struggle on their own, nor wait for other members of their network to join the app. This approach is already being followed by several organizations. For example, CryptoHarlem runs events dedicated to helping underserved and vulnerable communities improve their security and privacy, as well as avoid technology surveillance [19]. Future work should further investigate and codify best practices for such community-based activist trainings.

7 CONCLUSION

In this paper, we studied the types of digital security and privacy advice given to novice BLM protesters. In particular, we analyzed the advice given in 41 safety guides distributed on social media and the web during widespread BLM protests in spring 2020. We identified the most common types of advice, such as disabling phones' transmission features (e.g., putting them in airplane mode), communicating via an E2EE app, and disabling biometric unlocking on phones. While some of this advice is applicable outside of protest situations, other advice is fairly specific to in-person protests. Additionally, we conducted an online survey to investigate whether this advice is understood and used by 167 primarily novice BLM protesters. Unfortunately, survey respondents reported that they did not widely follow, nor fully understand, protest-specific recommendations, such as using E2EE apps instead of texting or disabling biometric phone unlocking. Further studies of in-person protesters' security and privacy needs are warranted. Future work should aim to develop improved safety guides for in-person protesters. These guides must better explain why certain advice offers key protections, as well as provide more detail on how to follow the advice.

ACKNOWLEDGMENTS

We thank Michelle Aninye, Weijia He, Jason Chee, and Ethan Waldman for their contributions to this project. We are grateful to our respondents for their thoughtful participation.

REFERENCES

[1] Monica Anderson, Skye Toor, Lee Rainie, and Aaron Smith. 2018. An analysis of #BlackLivesMatter and other Twitter hashtags related to political or social issues. *Pew Research Center* (2018).
[2] Ahmer Arif, Leo Graiden Stewart, and Kate Starbird. 2018. Acting the part: Examining information operations within #BlackLivesMatter discourse. *Proc. ACM Hum.-Comput. Interact.* 2 (2018).
[3] Ingolf Becker, Simon Parkin, and M. Angela Sasse. 2017. Finding security champions in blends of organisational culture. In *Proc. USEC*.
[4] Odette Beris, Adam Beautement, and M. Angela Sasse. 2015. Employee rule breakers, excuse makers and security champions: Mapping the risk perceptions and emotions that drive security behaviors. In *Proc. NSPW*.
[5] Black Lives Matter. 2020. About. https://blacklivesmatter.com/about/
[6] Black Lives Matter. 2020. Homepage. https://blacklivesmatter.com/
[7] Black Lives Matter Belfast. 2020. Safety guide. Twitter image. https://pbs.twimg.com/media/EZ1Onp7XkAACfFN.png.
[8] Black Lives Matter Seattle-King County. 2020. Safety while protesting: Protesting & supporting protests safely. Posted on Seattle Central College's Library. https://libguides.seattlecentral.edu/Staying_Safer_While_Rising_Up.
[9] Maia J. Boyd, Jamar L. Sullivan Jr., Marshini Chetty, and Blase Ur. 2021. Supplementary Materials for Understanding the Security and Privacy Advice Given to Black Lives Matter Protesters. https://www.blaseur.com/papers/chi21-blm-appendix.pdf
[10] Larry Buchanan, Quoctrung Bui, and Jugal K. Patel. 2020. Black Lives Matter may be the largest movement in U.S. history. New York Times. https://www.nytimes.com/interactive/2020/07/03/us/george-floyd-protests-crowd-size.html
[11] Karoline Busse, Julia Schäfer, and Matthew Smith. 2019. Replication: No one can hack my mind. Revisiting a study on expert and non-expert security practices and advice. In *Proc. SOUPS*.
[12] Frank Cain. 1983. *The Origins of Political Surveillance in Australia*. Angus & Robertson Sydney.
[13] Victoria Carty and Francisco G. Reynoso Barron. 2019. Social movements and new technology: The dynamics of cyber activism in the digital age. In *The Palgrave Handbook of Social Movements, Revolution, and Social Transformation*. Springer, 373–397.
[14] Garrett Chase. 2017. The Early History of the Black Lives Matter Movement, and the Implications Thereof. *Nevada Law Journal* 18 (2017), 1091.
[15] Ivan Cherapau, Ildar Muslukhov, Nalin Asanka, and Konstantin Beznosov. 2015. On the impact of Touch ID on iPhone passcodes. In *Proc. SOUPS*.
[16] Ward Churchill. 2001. To disrupt, discredit and destroy. *Liberation, Imagination, and the Black Panther Party* (2001), 93.
[17] Ward Churchill and Jim Vander Wall. 1990. The COINTELPRO papers. *Boston: South End* (1990).
[18] Sunny Consolvo, Jaeyeon Jung, Ben Greenstein, Pauline Powledge, Gabriel Maganis, and Daniel Avrahami. 2010. The Wi-Fi Privacy Ticker: Improving awareness & control of personal information exposure on Wi-Fi. In *Proc. UbiComp*.
[19] Joseph Cox. 2017. Matt Mitchell is arming underserved communities with anti-surveillance tools. Vice. https://www.vice.com/en_us/article/ezaane/matt-mitchell-is-arming-underserved-communities-with-anti-surveillance-tools
[20] David Cunningham and John A. Noakes. 2008. What if she's from the FBI? The effects of covert forms of social control on social movements. In *Surveillance and Governance: Crime Control and Beyond (Sociology of Crime Law and Deviance)*. Emerald Group Publishing Limited, 175–197.
[21] Duy Dang-Pham, Siddhi Pittayachawan, and Vince Bruno. 2017. Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace. *Computers in Human Behavior* 67 (2017), 196–206.
[22] Sauvik Das, Laura A. Dabbish, and Jason I. Hong. 2019. A typology of perceived triggers for end-user security and privacy behaviors. In *Proc. SOUPS*.
[23] Susie Day and Laura Whitehorn. 2001. Human rights in the United States: The unfinished story of political prisoners and COINTELPRO. *New Political Science* 23, 2 (2001), 285–297.
[24] Munmun De Choudhury, Shagun Jhaver, Benjamin Sugar, and Ingmar Weber. 2016. Social media participation in an activist movement for racial equality. In *Proc. ICWSM*.
[25] Lina Dencik and Jonathan Cable. 2017. The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. *International Journal of Communication* 11 (2017), 763–781.
[26] Mallika Dutt and Nadia Rasul. 2014. Raising digital consciousness: An analysis of the opportunities and risks facing human rights activists in a digital age. *Sur - International Journal on Human Rights* 20 (2014), 427.
[27] Ugo Etudo, Victoria Y. Yoon, and Niam Yaraghi. 2019. From Facebook to the streets: Russian troll ads and Black Lives Matter protests. In *Proc. HICSS*.
[28] Michael Fagan and Mohammad Maifi Hasan Khan. 2016. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In *Proc. SOUPS*.
[29] Deen Freelon, Charlton D. McIlwain, and Meredith D. Clark. 2016. Beyond the hashtags: #Ferguson, #Blacklivesmatter, and the online struggle for offline justice. https://cmsimpact.org/wp-content/uploads/2016/03/beyond_the_hashtags_2016.pdf
[30] Trevor Gabriel and Steven Furnell. 2011. Selecting security champions. *Computer Fraud & Security* 2011, 8 (2011), 8–12.
[31] Oscar H. Gandy. 2007. Data mining and surveillance in the post 9/11 environment. *The Surveillance Studies Reader* (2007), 147–157.
[32] Max Gedig. 2018. "Woke up with death every morning." Surveillance experiences of Black Panther Party activists. In *Surveillance, Race, Culture*. Springer, 267–281.
[33] Gunnar Harboe and Elaine M. Huang. 2015. Real-world affinity diagramming practices: Bridging the paper-digital gap. In *Proc. CHI*.

[34] Cormac Herley. 2009. So long, and no thanks for the externalities: The rational rejection of security advice by users. In *Proc. NSPW*.

[35] Alberto Hermida and Víctor Hernández-Santaolalla. 2018. Twitter and video activism as tools for counter-surveillance: The case of social protests in Spain. *Information, Communication & Society* 21, 3 (2018), 416–433.

[36] Kris Holt. 2020. 11 Ways To Protect Your Privacy While Protesting. Forbes. https://www.forbes.com/sites/krisholt/2020/06/07/privacy-black-lives-matter-protest-george-floyd/#70d382ce1801.

[37] Karen Holtzblatt and Hugh Beyer. 1997. *Contextual Design: Defining Customer-Centered Systems.* Elsevier.

[38] Jelani Ince, Fabio Rojas, and Clayton Davis. 2017. The social media response to Black Lives Matter: How Twitter users interact with Black Lives Matter through hashtag use. *Ethnic and Racial Studies* 40 (2017), 1814–1830.

[39] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "... no one can hack my mind": Comparing expert and non-expert security practices. In *Proc. SOUPS*.

[40] Sarah J. Jackson, Moya Bailey, and Brooke Foucault Welles. 2020. *# HashtagActivism: Networks of Race and Gender Justice.* MIT Press.

[41] Charles E. Jones. 1988. The political repression of the Black Panther Party 1966-1971: The case of the Oakland Bay Area. *Journal of Black Studies* 18, 4 (1988), 415–434.

[42] Esther Kim. 2020. Protesting tips for being safe and strong + #blacklivesmatter. Instagram post. https://www.instagram.com/p/CA6XErjhp2c/.

[43] Ken Klippenstein. 2019. FBI strategy guide FY2018-20 and threat guidance for racial extremists. https://www.scribd.com/document/421166393/FBI-Strategy-Guide-FY2018-20-and-Threat-Guidance-for-Racial-Extremists

[44] Kirk Kristofferson, Katherine White, and John Peloza. 2014. The nature of slacktivism: How the social observability of an initial act of token support affects subsequent prosocial action. *Journal of Consumer Research* 40, 6 (2014), 1149–1166.

[45] Yu-Hao Lee and Gary Hsieh. 2013. Does slacktivism hurt activism? The effects of moral balancing and consistency in online activism. In *Proc. CHI*.

[46] David Lyon. 2006. Airport screening, surveillance, and social sorting: Canadian responses to 9/11 in context. *Canadian Journal of Criminology and Criminal Justice* 48, 3 (2006), 397–411.

[47] David Lyon. 2007. Surveillance, security and social sorting: Emerging research priorities. *International Criminal Justice Review* 17, 3 (2007), 161–170.

[48] Gary Marx. 1974. Thoughts on a neglected category of social movement participant: The agent provocateur and the informant. *Amer. J. Sociology* 80 (1974).

[49] Alexandra Mateescu, Douglas Brunton, Alex Rosenblat, Desmond Patton, Zachary Gold, and danah boyd. 2015. Social media surveillance and law enforcement. *Data & Civil Rights* 27 (2015), 2015–2027.

[50] Dennis McCafferty. 2011. Activism vs. slacktivism. *Commun. ACM* 54, 12 (2011), 17–19.

[51] John G McNutt. 2018. *Technology, Activism, and Social Justice in a Digital Age.* Oxford University Press.

[52] Torin Monahan. 2006. Counter-surveillance as political intervention? *Social Semiotics* 16, 4 (2006), 515–534.

[53] Marcia Mundt, Karen Ross, and Charla M. Burnett. 2018. Scaling social movements through social media: The case of Black Lives Matter. *Social Media + Society* 4, 4 (2018).

[54] Deborah Netburn. 2012. YouTube's new face-blurring tool designed to protect activists. Los Angeles Times. https://www.latimes.com/business/la-xpm-2012-jul-18-la-fi-tn-youtube-face-blurring-20120718-story.html

[55] Huey P. Newton. 1980. *War Against the Panthers: A Study of Repression in America.* Vol. 1980. University of California, Santa Cruz.

[56] James Nicholson, Lynne Coventry, and Pamela Briggs. 2019. "If it's important it will be a headline" Cybersecurity information seeking in older adults. In *Proc. CHI*.

[57] Ihudiya Finda Ogbonnaya-Ogburu, Angela D.R. Smith, Alexandra To, and Kentaro Toyama. 2020. Critical race theory for HCI. In *Proc. CHI*.

[58] Eyal Peer, Laura Brandimarte, Sonam Somat, and Alessandro Acquisti. 2017. Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. In *Journal of Experimental Social Psychology*.

[59] Hao Peng, Ceren Budak, and Daniel M. Romero. 2019. Event-driven analysis of crowd dynamics in the Black Lives Matter online social movement. In *Proc. WWW*.

[60] James Pierce, Sarah Fox, Nick Merrill, and Richmond Wong. 2018. Differential vulnerabilities and a diversity of tactics: What toolkits teach us about cybersecurity. *Proc. ACM Hum.-Comput. Interact.* 2 (Nov. 2018).

[61] Prolific. 2020. Quickly find research participants you can trust. https://www.prolific.co/

[62] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as informal lessons about security. In *Proc. SOUPS*.

[63] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2016. How I learned to be secure: A census-representative survey of security advice sources and behavior. In *Proc. CCS*.

[64] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2019. How Well Do My Results Generalize? Comparing Security and Privacy Survey Results from MTurk, Web, and Telephone Samples. In *Proc. IEEE S&P*.

[65] Elissa M. Redmiles, Amelia R. Malone, and Michelle L. Mazurek. 2016. I think they're trying to tell me something: Advice sources and selection for digital security. In *Proc. IEEE S&P*.

[66] Elissa M. Redmiles, Miraida Morales, Lisa Maszkiewicz, Rock Stevens, Everest Liu, Dhruv Kuchhal, and Michelle L. Mazurek. 2018. First steps toward measuring the readability of security advice. In *Proc. ConPro*.

[67] Elissa M. Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L. Mazurek. 2020. A comprehensive quality evaluation of security and privacy advice on the web. In *Proc. USENIX Security*.

[68] Robert W. Reeder, Iulia Ion, and Sunny Consolvo. 2017. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security & Privacy* 15, 5 (2017), 55–64.

[69] Katelyn Ringrose and Divya Ramjee. 2020. Watch where you walk: Law enforcement surveillance and protester privacy. *California Law Review* 11, 349 (2020).

[70] Ellen Schrecker. 2004. *Threatening Anthropology: McCarthyism and the FBI's Surveillance of Activist Anthropologists.* Duke University Press.

[71] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. 2007. Anti-phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. In *Proc. SOUPS*.

[72] Daniel J. Solove. 2007. I've got nothing to hide and other misunderstandings of privacy. *San Diego L. Rev.* 44 (2007), 745.

[73] Alice Speri. 2015. 1 2014 8:14 Silent vigil alert #NMOS14. The Intercept. https://assets.documentcloud.org/documents/2178934/1-2014-8-14-silent-vigil-alert-nmos14.pdf

[74] Katta Spiel, Oliver L. Haimson, and Danielle Lottridge. 2019. How to do better with gender on surveys: A guide for HCI researchers. *Interactions* 26, 4 (2019), 62–65.

[75] Kate Starbird. 2019. Disinformation's spread: Bots, trolls and all of us. *Nature* 571, 7766 (2019), 449–450.

[76] Leo Graiden Stewart, Ahmer Arif, A. Conrad Nied, Emma S. Spiro, and Kate Starbird. 2017. Drawing the lines of contention: Networked frame contests within# BlackLivesMatter discourse. *Proc. ACM Hum.-Comput. Interact* 1 (2017).

[77] Leo Graiden Stewart, Ahmer Arif, and Kate Starbird. 2018. Examining trolls and polarization with a retweet network. In *Proc. MIS2*.

[78] Reem Talhouk, Kellie Morrissey, Sarah Fox, Nadia Pantidi, Emma Simpson, Lydia Emma Michie, and Madeline Balaam. 2018. Human computer interaction & health activism. In *Proc. CHI EA*.

[79] Alvin B. Tillery. 2019. What kind of movement is Black Lives Matter? The view from Twitter. *Journal of Race, Ethnicity and Politics* 4, 2 (2019), 297–323.

[80] Twitter. 2020. Protesting safely. Twitter image. https://pbs.twimg.com/media/EZZ0-koUEAAazF3.jpg.

[81] Marlon Twyman, Brian C. Keegan, and Aaron Shaw. 2017. Black Lives Matter in Wikipedia: Collective memory and collaboration around online social movements. In *Proc. CSCW*.

[82] Julie Uldam. 2016. Corporate management of visibility and the fantasy of the post-political: Social media and surveillance. *New Media & Society* 18, 2 (2016), 201–219.

[83] Julie Uldam. 2018. Social media visibility: challenges to activism. *Media, Culture & Society* 40, 1 (2018), 41–58.

[84] Peter Ullrich and Philipp Knopp. 2018. Protesters' reactions to video surveillance of demonstrations: Counter-moves, security cultures, and the spiral of surveillance and counter-surveillance. *Surveillance & Society* (2018).

[85] Elham Vaziripour, Justin Wu, Mark O'Neill, Jordan Whitehead, Scott Heidbrink, Kent Seamons, and Daniel Zappala. 2017. Is that you, Alice? A usability study of the authentication ceremony of secure messaging applications. In *Proc. SOUPS*.

[86] Kevin Walby and Jeffrey Monaghan. 2011. Private eyes and public order: Policing and surveillance in the suppression of animal rights activists in Canada. *Social Movement Studies* 10, 1 (2011), 21–37.

[87] Rick Wash. 2010. Folk models of home computer security. In *Proc. SOUPS*.

[88] Rick Wash and Molly M. Cooper. 2018. Who provides phishing training? Facts, stories, and people like me. In *Proc. CHI*.

[89] Denise J. Wilkins, Andrew G. Livingstone, and Mark Levine. 2019. Whose tweets? The rhetorical functions of social media use in developing the Black Lives Matter movement. *British Journal of Social Psychology* 58, 4 (2019), 786–805.

[90] Dean Wilson and Tanya Serisier. 2010. Video activism and the ambiguities of counter-surveillance. *Surveillance & Society* 8, 2 (2010), 166–180.

[91] William Lafi Youmans and Jillian C. York. 2012. Social media and the activist toolkit: User agreements, corporate interests, and the information infrastructure of modern social movements. *Journal of Communication* 62, 2 (2012), 315–329.

[92] Mihir Zaveri. 2020. 'I need people to hear my voice': Teens protest racism. New York Times. https://www.nytimes.com/2020/06/23/us/teens-protest-black-lives-matter.html

[93] Weiyu Zhang. 2013. Redefining youth activism through digital technology in Singapore. *International Communication Gazette* (2013).