Protest Privacy Recommendations: An Analysis of Digital Surveillance Circumvention Advice During Black Lives Matter Protests

Kandrea Wade
kandrea.wade@colorado.edu
University of Colorado Boulder
Boulder, Colorado, USA

Jed R. Brubaker
jed.brubaker@colorado.edu
University of Colorado Boulder
Boulder, Colorado, USA

Casey Fiesler
casey.fiesler@colorado.edu
University of Colorado Boulder
Boulder, Colorado, USA

ABSTRACT

This paper describes a qualitative study of media and advocacy publications about digital surveillance in the context of Black Lives Matter protests, including recommendations for techniques on how to circumvent such surveillance. We conducted a content analysis of the recommendations given for circumventing surveillance provided by media, news, activist, and commercial outlets. We describe the recommendations provided and identify common fears and implications of protest surveillance as expressed by these sources. We identified thematic categories of surveillance fears and implications, including ruined reputations, online harassment, arrest, lack of transparency, and the chilling of free speech and protest. Finally, we describe what we see as challenges protesters will have implementing the recommendations (for example, due to availability and accessibility of technology and certain types of expertise required), complicating the creation of the kind of security culture protesters need.

CCS CONCEPTS

• **Human-centered computing**; • **Security and privacy → Human and societal aspects of security and privacy**;

KEYWORDS

Black Lives Matter, protest, surveillance, circumvention, privacy, digital, safety, protection, literacy, security

ACM Reference Format:
Kandrea Wade, Jed R. Brubaker, and Casey Fiesler. 2021. Protest Privacy Recommendations: An Analysis of Digital Surveillance Circumvention Advice During Black Lives Matter Protests. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI '21 Extended Abstracts), May 8–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3411763.3451749

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
CHI '21 Extended Abstracts, May 8–13, 2021, Yokohama, Japan
© 2021 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-8095-9/21/05…$15.00
https://doi.org/10.1145/3411763.3451749

1 INTRODUCTION & BACKGROUND

As demonstrations against injustice such as Black Lives Matter protests have continued to grow, so have concerns about the use of surveillance technologies by government and policing agencies and the risks these technologies pose for individuals who choose to participate in protests. Within this active resistance, activist organizations and individual protesters are taking it upon themselves to re-engineer and rethink how these technologies are used to make them work in their favor, with the goal of achieving digital privacy in public spaces [16, 25]. Currently, device abandonment and/or memory clearing, encrypted communication services such as Signal, and disabling location tracking are among the tactics used by protesters to support and protect on-the-ground efforts. Research has shown that groups with similar values and concerns about being targeted or compromised are participating in "security culture", taking it upon themselves to actively resist and circumvent the gaze of surveillance technologies through "methods and resources" specific to that group [36]. We are using Ullrich and Knopp's definition of security culture to "designate established movement or group specific norms and sets of practices intended to secure political agency under conditions of perceived threats." Using this designation, Black Lives Matter would be considered a "movement-specific security culture", where the need and tactics for circumventing surveillance are specific to the participants of Black Lives Matter protests [42, 45]. The security culture specific to these individuals and groups of protesters is keeping people safe despite the efforts made to establish systems of tracking, identification, and classification [36, 37]. Civilians are leading efforts to disrupt and intervene in surveilling technologies to protect the messages of equality, such as "eradicating white supremacy and countering acts of [racialized] violence" [28], and those delivering them.

The threats to these groups are real and tangible. Drone imaging for identification, tower interference for intercepting messages, property seizure and device scraping for data collection (contact tracing), spoofed social media accounts for monitoring/observing, city cameras for tracking (license plates and contact tracing), and many other techniques have led to imprisonment, misidentification, and collateral damage that comes with being surveilled [36–38]. Efforts made by government and policing agencies to impede collective action can eliminate agency and visibility in the struggle and fight for change, potentially silencing those who are already marginalized.

Focusing on the novel needs of these established yet vulnerable groups, such as Black Lives Matter protesters, also provides a window into broader needs for enhanced security, privacy, and

communications. This paper describes an investigation into potential strategies that protesters might use to protect themselves, and how these strategies reflect the potential harms of surveillance. The study will provide valuable insight into, and for, marginalized and vulnerable groups by pinpointing the need for technologies specialized to these groups and identifying a new market segment that needs tailored tools. As a person of color who is invested in collective action and organization, the first author is directly connected to and affected by the risks and implications that come from the digital surveillance of protest groups and similar vulnerable communities. We are conducting this work to protect and serve individuals within marginalized communities and to help lead to a greater voice, choice, venue, and access to be able to request and create technologies tailored to their needs.

In recognition of the growing concern regarding privacy for protesters, various media outlets, as well as organizations such as the American Civil Liberties Union (ACLU), have developed lists of recommendations and strategies for protecting oneself from protest surveillance [2, 12, 19]. Such recommendations not only illustrate what strategies are seen as effective for counteracting surveillance in this context, but they also reflect the underlying fears and potential harms such strategies are intended to mitigate. With an eye towards mapping out the landscape of surveillance fears, harms, advice, and strategies we looked to these sources of information available to protesters.

We conducted a content analysis of the recommendations given for circumventing surveillance and communicating messages as they are offered by media, news, activist, and commercial outlets. The purpose of this work is to describe the recommendations provided by an array of resources, identify the common fears and implications of protest surveillance as expressed by these sources, and explore the relationship between the recommendations given and what impact they may realistically make for protesters. We chose to focus specifically on Black Lives Matter protests due to the timeliness, relevance and current discussions taking place among the institutions that currently create and use surveillance technologies, in addition to the groups that are at risk of being surveilled. Based on our findings, we also speculate about how effective these publicly available privacy solutions may be for Black Lives Matter protesters and other activists. This study aims to identify patterns, standards and themes to the recommendations given, and gain a deeper understanding of collective surveillance resistance behavior [27].

With these goals in mind, our research questions are: (1) What strategies for surveillance circumvention are the media, activist groups, and other sources providing to protesters? and (2) What do those strategies suggest about the underlying problems and/or people's fears? Based on the answers to these questions as seen in our data, we also speculate about how useful these recommendations actually are for protesters.

2 METHODS

To examine the recommendations given to protesters for surveillance circumvention, we collected a dataset in June 2020 of 27 articles and media publications that contain recommendations about how to circumvent surveillance at Black Lives Matter protests. Our goals were to map surveillance fears and perceived harms, examine the recommendations for surveillance circumvention given by the sources, and create a framework for more considerations and context to be provided when suggesting methods for circumvention.

We identified publications by searching for key phrases on Google Search, Google News, and YouTube. Based on concepts from existing literature on security culture and surveillance [2, 27, 36] and on an informal review of trending news coverage of protests during June 2020 (e.g., [2, 5, 10, 15, 19, 26]), we chose the following keywords for our search: *protest surveillance, protester protection, protest privacy, Black Lives Matter surveillance, how to stay/staying safe at protests, digital privacy at protests*, and *protest surveillance circumvention*. The analysis for this dataset was conducted by compiling the explicitly stated fears and implications from these publications and organizing them into five high level themes. Additionally, the suggestions listed were analyzed as a way of looking at what fears and implications they imply, which may be inline or vary from what was explicitly listed.

Our search yielded over 60 publications, which the first author then filtered using the following inclusion criteria: (1) addressed at least one keyword, (2) specifically focused on protests or digital privacy in public, and (3) explicitly mentioned fears, implications, or recommendations for surveillance circumvention. The final dataset included 27 publications; 22 of these publications included recommendations, while 22 enumerated fears and implications of surveillance technology, and 17 articles included both types of information. Details of the dataset can be seen in Table 1.

Next, we classified the type of outlet that published each article according to Wikipedia's definitions of major news sources, first separating the news sources from media (blogs and online magazines) and then listing each other source according to its type [48]. Our dataset included articles from news (8), activist groups (7), product descriptions (2), and other media (10) such as blogs and online editions of magazines. We then turned our analysis to the specific recommendations in these publications. We started by extracting recommendations, resulting in 30 unique recommendations. We grouped these recommendations into higher level categories and recorded frequencies.

Using Braun and Clarke's six phases of thematic analysis [7], our qualitative analysis was conducted by first becoming familiar with the data, paying specific attention to patterns. The first author conducted the coding and all authors discussed emerging codes and themes during the analysis process. We generated the initial codes by collapsing the data on the listed fears and implications and making inferences about what the codes mean. We then combined the codes into overarching themes and moved into phase 4 where we looked at how the themes support the data. Next, the authors defined what each theme is, concluding with checking back to ensure that the descriptions were an accurate representation of the data.

Derived from our thematic analysis, we found that the guidelines and advice given by the sources imply five types of fears, including: ruined reputations, online harassment, arrest, lack of transparency, and free speech chilling/killing protest. Additionally, we found that there are issues of accessibility and validity that come with the recommendations provided by these sources.

Table 1: Publications.

Source/Label	Date	Title	Recs	Fears/Impls.
ACLU-1[1]	6/27/2020*	Spying on Protesters		X
ACLU-2[2]	6/3/2020	How do you protect your privacy at a protest?	X	X
Amnesty International[35]	6/12/2020	Tactics to secure your smartphone before joining a protest	X	X
CNBC[14]	6/13/2020	We don't know how people are being surveilled		X
CNET-1[32]	6/9/2020	Police body cameras at protests raise privacy concerns		X
CNET-2[30]	6/17/2020	Protesting Tips: What to bring, what not to bring and how to protect yourself	X	
CNN-1[3]	6/3/2020	If you're planning to take part in protests, know your rights. Read this.	X	X
CNN-2[31]	6/12/2020	US Government spy planes monitored George Floyd protests		X
Consumer Reports[15]	6/3/2020	How to protest phone privacy at a protest	X	X
EFF-1[4]	6/4/2020	Protecting your privacy if your phone is taken away	X	X
EFF-2[39]	6/8/2020	You have a First Amendment Right to record the police	X	
EPIC[9]	6/18/2020	Protester Privacy and Free Expression of Rights	X	X
Forbes-1[19]	6/8/2020	11 Ways to Protect Your Privacy While Protesting	X	X
Forbes-2[8]	6/11/2020	Microsoft Urged to Follow Amazon and IBM		X
The Intercept[24]	4/21/2017	Cybersecurity for the People: How to Protect Your Privacy at a Protest	X	X
The Markup[46]	6/4/2020	How Do I Prepare My Phone for Protest?	X	X
Mission Darkness[13]	6/27/2020*	Mission Darkness Window Faraday Bags for phones	X	
NPR[29]	6/28/2020	Should Images of Protesters Be Blurred to Protect Them From Retribution?	X	
Popular Mechanics[26]	6/4/2020	The 3 Things You Must Do to Protect Your Privacy While Protesting	X	X
Privacy International[20]	6/15/2020	Ethnic minorities at greater risk of oversurveillance after protests		X
Silent Pocket[34]	6/5/2020	Privacy and Security While Protesting	X	
Time[5]	6/1/2020	Going to a Protest? Here's How to Protect Your Digital Privacy	X	X
The Verge[10]	6/4/2020	How to secure your phone before attending a protest	X	X
Vice[12]	6/1/2020	How to Protest Without Sacrificing Your Digital Privacy	X	X
Washington Post-1[23]	6/3/2020	America is awash in cameras, a double-edged sword for protesters and police	X	X
Washington Post-2[11]	6/3/2020	Your Protest is Being Watched. Here's How to Protect Your Privacy	X	X
Wired[17]	5/31/2020	How to Protest Safely in the Age of Surveillance	X	X

* No publication date provided. Listed date is the date on which the article was accessed.

3 MAPPING STRATEGIES, FEARS & PERCEIVED HARMS

In this section we describe the recommended strategies we identified through our analysis, as well as themes of implied fears and perceived harms of protest surveillance. Quotes that come from sources in our dataset are indicated by the label contained in Table 1.

3.1 Recommended Strategies

We found 30 types of recommendations in the sources described above. The most popular included: disable biometric unlocking (which appeared in 63.6% of the sources containing recommendations), use encrypted messaging/calls (59.1%), complicated passwords (50%), airplane mode (50%), bring no phone (45.5%), turn off location (45.5%), and manage metadata (31.8%).

While analyzing these recommendations, we also considered why some recommendations might be listed more frequently than others. It is worth noting that, other than simply informing the reader of a suggestion and its purpose, very rarely did sources provide any validation or reasoning for the recommendations they made. For example, many of the solutions provided focus on avoiding identification via facial recognition. However, few sources provided any information about how facial recognition technology works, why it is such a threat, and how and whether these techniques are successful in protecting people from it.

These recommendations imply certain fears and perceived harms, though many sources were explicitly in detailed fears and harms as well. Next, we describe the themes that emerged from our analysis of both these recommendations and the broader commentary included in these sources.

3.2 Fears & Perceived Harms

Ruined Reputation. The fear of ruined reputation is situated in the suspicion that once an individual is identified at a protest, they will potentially have that association follow them for the rest of their lives, potentially affecting future jobs, relationships, and other interactions with individuals or organizations that do not agree with the behavior of the individual or the message being promoted within the protest. For example, an article from CNBC stated that "Surveillance and facial recognition data can be connected to many other pieces of information by government agencies and marketers... With the right tools, that data can easily be matched to social media

profiles, criminal histories, and credit reports" [CNBC], leading to potentially longer lasting farther reaching effects of participating in a protest.

Harassment. According to our data, the advice given also reflects that protest participants "don't necessarily want [their] participation in a demonstration to follow [them] around or lead to harassment online" [Vice]. Online harassment falls in line with the first fear of a reputation following a protester, but also goes deeper when considerations are made for how surveilling agents have been found to create fake social media profiles to attempt to befriend protesters to investigate their tactics of organization and surveillance circumvention [38]. These online and in-person interactions have, at times, led to direct harassment by surveilling entities and those who generally disagree with the tactics and initiatives of protesters.

Arrest. The sources claimed that the fear of arrest through identification was valid during a protest as much as it was after. "Information gathered through digital surveillance has been introduced in situations where protesters have been prosecuted" [Consumer Reports], contributing to the fear of arrest for attending or being in connection with a protest. The lingering effects of identification cause protesters, as the sources in the dataset report, to fear that even though they were not arrested during the protest, their actions, behaviors, and identities could be captured through surveillance, leading to future arrests or legal actions being taken by authorities. The technologies used to surveil protesters are also varied and multi-leveled with "authorities in many jurisdictions are using facial recognition systems and other technology to identify protesters" [Forbes-2], among other camera, recording and signal interfering tech. Considering that "any evidence placing people at protests could be enough to get them arrested" [Verge], any involvement in the planning or attendance of a protest is considered to be behavior that could put an individual at risk for future action by law enforcement.

Lack of Transparency. Protesters also have no real transparency or understanding of what is being done with the information that is being collected via surveillance. In our data, CNBC mentions that "what exactly that data [collected from surveillance of protesters] will be used for, no one really knows yet. Activists and privacy researchers say that's the problem" [CNBC]. We found that sources claim there is a fear that once the identity of an individual has been associated with efforts of organization and protest, in what the surveilling entities would see as an unlawful or unrestful manner, that the individual and anyone they are found to associate with through contact tracing could be subject to further investigation, surveillance and tracking, with the intention of preventing or interfering with future plans to organize or resist authority.

Chill Speech & Protest. Finally, we found concerns about First Amendment rights and the potential for surveillance to chill free speech and dissuade collective action and organization altogether. The fear is centered around the threat of potential legal action being taken against protesters being enough to stop them from organizing before it begins, hindering an essential right and letting the issues being protested against remain unaddressed. In our data CNN mentions that "surveillance challenges the right to organize as it hinders and impedes collective action, becoming a 'deep and profound' breach of Americans' First and Fourth Amendment rights" [CNN]. The ethical concerns of preventing protest are becoming more prevalent in relation to digital surveillance, as this was one of the more commonly mentioned fears with Forbes, CNN, EPIC, CNBC, CNET all reporting on the topic with advice from various activist leaders and groups.

Each of these fears and implications have the potential to impact the individuals involved in protests, but more investigation is needed to discover how much of these fears are shared by the protesters themselves.

4 CHALLENGES FOR A PROTEST SECURITY CULTURE

Now that we have mapped the strategies, fears, and perceived harms, we now discuss further implications and what we see as the challenges that protesters might have in implementing the recommendations made and creating the kind of security culture they need.

Lack of Appropriate Technology. One issue that emerged from our findings was a potential lack of existing technology required by protesters to appropriately protect themselves while also allowing for connection or reporting out. In our dataset, the Washington Post notes the rise in popularity of documenting what is happening on the ground and reporting out to the public in real time, but we found that it is difficult for protesters to complete such tasks without fear of the public networks they are using being tapped or interfered with to locate the individual or prevent/stop the transmission. Additionally, in line with organization efforts, protesters often find a need to communicate among themselves for mapping, safety, emergency, and various other reasons. With their communications, again, traveling over potentially compromised networks, there are currently no completely safe methods for those on the ground to be able to connect. These protester needs call for technological devices that do not currently exist but are in the process of being developed such as Faraday bags (mentioned by Mission Darkness and Silent Pocket) specifically for protesters and other commercial products that are intended for surveillance circumvention at large gatherings.

Complicated Solutions/Accessibility Issues. Most of the recommendations would require additional knowledge of personal devices. Though potentially effective, some of the recommendations given may be more effective or reasonable to comprehend for those who may be more experienced and knowledgeable with protests or with technology. Recommendations given for circumventing surveillance, especially those that involve a more in-depth understanding of hardware, software, systems, and networks, may not apply to less technologically adept users. Therefore, it was not surprising to see that the more complicated and technologically involved the recommendations (e.g., VPNs, permission managers, and device encryption) the less they appeared in our data. Some sources did provide some explanation for these complex recommendations or linked to outside information. However, the level of detail provided was not consistent, and it is likely that the instructions may be difficult to follow for people with less technical literacy.

Additionally, though some sources provided instructions (or links to them) for Apple and Android devices, recommendations may not be universally applicable for users without devices that fall under

these major brands or that may be older, previous generations of technology. Our analysis reveals an expectation of high levels of digital literacy for protesters and raises more questions of who these specific recommendations are meant for, and who they would best be suited for. What if the more technologically advanced solutions are actually the most effective but not as accessible or attainable for the average protester? The potential here is that some who may need these recommendations more than others are not privy to the same information due to their level of digital literacy. For example, with 21% of the protest attendees being over the age of 50 [6], there is likely a lower level of understanding and accessibility that some of these more advanced recommendations provide. Though individuals over 50 are closing the technological gap more than ever with owning or buying devices at a rate that is competitive with younger generations [21], there is not enough research conducted on how well this age group understands the features of their devices and how in depth they can, or are willing to, go in taking all of the suggested measures to keep them safe from surveillance. We also do not know how accessible these more advanced recommendations are for individuals with varying levels of physical or cognitive abilities.

5 FUTURE WORK

Our analysis revealed themes of fears and implications surrounding protest surveillance, including potential issues with the helpfulness of recommendations, leading to questions that can only be answered by protesters themselves through further research. For example, our findings open up questions related to protester privacy concerns, privacy and digital literacy, adaptations of existing ICT (Information and Communication Technologies) for demonstrations, and most popular and effective techniques.

Issues like surveillance circumvention at protests require those with on the ground, first-hand experience to be fully and truly studied. It is in these realms that those with high accolades and levels of power, such as researchers and technology developers, mean little to nothing compared to what has been experienced, embodied, and lived by the lay person, in this case, the protester [18]. The ability to speak to these audiences with such levels of efficiency, specificity, and reach is significant to study in the way that we, as researchers and developers, could learn how to successfully address previously untapped audiences at their most significant moments of need. In our continuing work, we hope to conduct interviews, with the goal of providing visibility for what these internal, folk threat models and values within protester "security culture" are, what technologies are being used on the ground and how, what technological developments could be made to serve these groups better, and how to facilitate more collaborative and reciprocal relationships between the users and developers in the future [40]. We also hope to uncover what roles that the participants in these movements may be playing in efforts to create some semblance of organized, collective action and planning through technological interventions [22, 41, 43, 44, 47]. This further work can aid in establishing patterns and standards to the methods utilized and modeling collective and surveillance resistant behavior [27, 33].

We also note that as we and others continue to investigate this important topic, such research requires careful ethical consideration. For example, revealing the tactics and methods of surveillance circumvention might put a vulnerable group at even more risk, but at the same time, could help them to have a representation, creating a tension between the motivation and the gain of the research. Precautions should be taken to protect the identities and specific methods of surveillance circumvention by these individuals and groups, while in reporting being as factual, ethical, and forthright with all parties as possible.

6 CONCLUSION

Protesters, along with other vulnerable groups, should have access to relevant, practical, effective, and feasible solutions to protect their privacy at demonstrations and other activities involving collective action. More research needs to be conducted to fully investigate and validate if the recommendations given to protesters are actually working to assist in circumventing surveillance. The findings of our research currently conclude that outside of preventing facial recognition and phones from being accessed after arrest, many sources are quite varied and span many different recommendations, making it difficult for the average protest attendee to obtain a full understanding on what might be the best tactics of obfuscation for them and why.

REFERENCES

[1] ACLU. [n.d.]. Spying on Protesters. *American Civil Liberties Union* ([n. d.]). https://www.aclu.org/issues/free-speech/rights-protesters/spying-protesters

[2] ACLU. 2020. How Do You Protect Your Privacy At A Protest? *ACLU-YouTube* (Jun 2020). https://www.youtube.com/watch?v=HJkVko8dHys

[3] Scottie Andrew. 2020. If you're planning to take part in protests, know your rights. Read this. *CNN* (Jun 2020). https://www.cnn.com/2020/06/02/us/how-to-protest-safely-know-your-rights-wellness-trnd/index.html

[4] Andrés Arrieta. 2020. Protecting your privacy if your phone is taken away. (Jun 2020). https://www.eff.org/deeplinks/2020/06/protecting-your-privacy-if-your-phone-taken-away

[5] Patrick Lucas Austin. 2020. Going to a Protest? How to Protect Your Digital Privacy. *Time* (Jun 2020). https://time.com/5852009/protest-digital-privacy/.

[6] Amanda Barroso and Rachel Minkin. 2020. Recent protest attendees are more racially and ethnically diverse, younger than Americans overall. *Pew Research Center* (Aug 2020). https://www.pewresearch.org/fact-tank/2020/06/24/recent-protest-attendees-are-more-racially-and-ethnically-diverse-younger-than-americans-overall/

[7] Virginia Braun and Victoria Clarke. 2013. *Successful qualitative research: A practical guide for beginners*. sage.

[8] Thomas Brewster. 2020. Microsoft Urged To Follow Amazon And IBM: Stop Selling Facial Recognition To Cops After George Floyd's Death. *Forbes* (Jun 2020). https://www.forbes.com/sites/thomasbrewster/2020/06/11/microsoft-urged-to-follow-amazon-and-ibm-stop-selling-facial-recognition-to-cops-after-george-floyds-death/

[9] Electronic Privacy Information Center. [n.d.]. EPIC - Protestor Privacy and Free Expression Rights. *Electronic Privacy Information Center* ([n. d.]). https://epic.org/privacy/protest/

[10] Aliya Chaudhry. 2020. How to secure your phone before attending a protest. *The Verge* (Jun 2020). https://www.theverge.com/21276979/phone-protest-demonstration-activism-digital-how-to-security-privacy

[11] James Cornsilk and Jonathan Baran. 2020. Your protest is being watched. Here's how to protect your privacy. https://www.washingtonpost.com/video/technology/your-protest-is-being-watched-heres-how-to-protect-your-privacy/2020/06/03/3badf963-ef49-47f9-8228-2d8bfb8c88b3_video.html

[12] Joseph Cox and Lorenzo Franceschi-Bicchierai. 2020. How to Protest Without Sacrificing Your Digital Privacy. *VICE* (Jun 2020). https://www.vice.com/en/article/gv59jb/guide-protect-digital-privacy-during-protest

[13] MOS Equipment. [n.d.]. Mission Darkness™ Window Faraday Bag for Phones. *MOS Equipment* ([n. d.]). https://mosequipment.com/products/mission-darkness-small-window-faraday-bag

[14] Lauren Feiner. 2020. We don't know how protests are being surveilled. Here's why that's a problem. *CNBC* (Jun 2020). https://www.cnbc.com/2020/06/13/researchers-politicians-call-for-transparency-in-protest-surveillance.html

[15] Thomas Germain. 2020. How to Protect Phone Privacy and Security During a Protest. *Consumer Reports* (Jun 2020). https://www.consumerreports.org/privacy/protect-phone-privacy-security-during-a-protest/

[16] Sucheta Ghoshal, Rishma Mendhekar, and Amy Bruckman. 2020. Toward a grassroots culture of technology practice. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW1 (2020), 1–28.

[17] Andy Greenberg and Lily Newman. 2020. How to Protest Safely in the Age of Surveillance. *Wired* (May 2020). https://www.wired.com/story/how-to-protest-safely-surveillance-digital-privacy/

[18] Reiner Grundmann. 2017. The problem of expertise in knowledge societies. *Minerva* 55, 1 (2017), 25–48.

[19] Kris Holt. 2020. 11 Ways To Protect Your Privacy While Protesting. *Forbes* (Jun 2020). https://www.forbes.com/sites/krisholt/2020/06/07/privacy-black-lives-matter-protest-george-floyd/.

[20] Privacy International. 2020. Ethnic minorities at greater risk of oversurveillance after protests. *Privacy International* (Jun 2020). http://privacyinternational.org/news-analysis/3926/ethnic-minorities-greater-risk-oversurveillance-after-protests

[21] Brittne Nelson Kakulla. 2020. 2020 Tech Trends of the 50+. *AARP* (Jan 2020). https://www.aarp.org/research/topics/technology/info-2019/2020-technology-trends-older-americans.html

[22] Andrea Kavanaugh, Steven D Sheetz, Riham Hassan, Seungwon Yang, Hicham G Elmongui, Edward A Fox, Mohamed Magdy, and Donald J Shoemaker. 2013. Between a rock and a cell phone: Communication and information technology use during the 2011 uprisings in Tunisia and Egypt. *International Journal of Information Systems for Crisis Response and Management (IJISCRAM)* 5, 1 (2013), 1–21.

[23] Heather Kelly and Rachel Lerman. 2020. America is awash in cameras, a double-edged sword for protesters and police. *The Washington Post* (Jun 2020). https://www.washingtonpost.com/technology/2020/06/03/cameras-surveillance-police-protesters/

[24] Micah Lee and Lauren Feeney. 2017. Cybersecurity for the People: How to Protect Your Privacy at a Protest. *The Intercept* (Apr 2017). https://theintercept.com/2017/04/21/cybersecurity-for-the-people-how-to-protect-your-privacy-at-a-protest/

[25] Hanlin Li, Nicholas Vincent, Janice Tsai, Jofish Kaye, and Brent Hecht. 2019. How Do People Change Their Technology Use in Protest? Understanding. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–22.

[26] Courtney Linder. 2020. The 3 Things You Must Do to Protect Your Privacy While Protesting. *Popular Mechanics* (Jun 2020). https://www.popularmechanics.com/technology/security/a32767037/protect-phone-privacy-security-protest/.

[27] Aaron K Martin, Rosamunde E Van Brakel, and Daniel J Bernhard. 2009. Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. *Surveillance & Society* 6, 3 (2009), 213–232.

[28] Black Lives Matter. 2020. Black Lives Matter-About. *Black Lives Matter* (Oct 2020). https://blacklivesmatter.com/about/

[29] Kelly McBride. 2020. Should Images Of Protesters Be Blurred To Protect Them From Retribution? *NPR* (Jun 2020). https://www.npr.org/sections/publiceditor/2020/06/18/879223467/should-images-of-protesters-be-blurred-to-protect-them-from-retribution

[30] Sarah Mitroff. 2020. How to protect yourself while protesting for the Black Lives Matter movement. *CNET* (Jun 2020). https://www.cnet.com/health/how-to-protect-yourself-from-coronavirus-at-black-lives-matter-protests/

[31] Pete Muntean and Gregory Wallace. 2020. US government spy planes monitored George Floyd protests. *CNN* (Jun 2020). https://www.cnn.com/2020/06/11/politics/spy-planes-george-floyd-protests/index.html

[32] Alfred Ng. 2020. Police body cameras at protests raise privacy concerns. *CNET* (Jun 2020). https://www.cnet.com/news/police-body-cameras-at-protests-raise-privacy-concerns/

[33] Stephen Owen. 2017. Monitoring social media and protest movements: ensuring political order through surveillance and surveillance discourse. *Social Identities* 23, 6 (2017), 688–700.

[34] Silent Pocket. 2020. Privacy And Security While Protesting. *Silent Pocket* (Jun 2020). https://silent-pocket.com/blogs/news/privacy-and-security-while-protesting

[35] Ramy Raoof. 2020. Tactics to secure your smartphone before joining a protest. *Amnesty International* (Jun 2020). https://www.amnesty.org/en/latest/campaigns/2020/06/tactics-to-secure-phone-before-a-protest/

[36] Pedro Sanches, Vasiliki Tsaknaki, Asreen Rostami, and Barry Brown. 2020. Under Surveillance: Technology Practices of those Monitored by the State. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–13.

[37] Morgan Klaus Scheuerman, Kandrea Wade, Caitlin Lustig, and Jed R Brubaker. 2020. How We've Taught Algorithms to See Identity: Constructing Race and Gender in Image Databases for Facial Analysis. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW1 (2020), 1–35.

[38] Jon Schuppe. 2018. Undercover cops break Facebook rules to track protesters, ensnare criminals. *NBCNews.com* (Oct 2018). https://www.nbcnews.com/news/us-news/undercover-cops-break-facebook-rules-track-protesters-ensnare-criminals-n916796

[39] Adam Schwartz and Sophia Cope. 2020. You Have a First Amendment Right to Record the Police. *Electronic Frontier Foundation* (Jun 2020). https://www.eff.org/deeplinks/2020/06/you-have-first-amendment-right-record-police

[40] Aaron Shaw, Haoqi Zhang, Andrés Monroy-Hernández, Sean Munson, Benjamin Mako Hill, Elizabeth Gerber, Peter Kinnaird, and Patrick Minder. 2014. Computer supported collective action. *interactions* 21, 2 (2014), 74–77.

[41] Emma S Spiro and Andrés Monroy-Hernández. 2016. Shifting stakes: Understanding the dynamic roles of individuals and organizations in social media protests. *PloS one* 11, 10 (2016), e0165387.

[42] Amory Starr, Luis A Fernandez, Randall Amster, Lesley J Wood, and Manuel J Caro. 2008. The impacts of state surveillance on political assembly and association: A socio-legal analysis. *Qualitative Sociology* 31, 3 (2008), 251–270.

[43] Ekaterina Stepanova. 2011. The role of information communication technologies in the "Arab Spring". *Ponars Eurasia* 15, 1 (2011), 1–6.

[44] Marie Truelove, Maria Vasardani, and Stephan Winter. 2014. Testing a model of witness accounts in social media. In *Proceedings of the 8th workshop on geographic information retrieval*. 1–8.

[45] 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. (2018).

[46] Maddy Varner. 2020. *How Do I Prepare My Phone for a Protest? – The Markup* (Jun 2020). https://themarkup.org/ask-the-markup/2020/06/04/how-do-i-prepare-my-phone-for-a-protest

[47] Onur Varol, Emilio Ferrara, Christine L Ogan, Filippo Menczer, and Alessandro Flammini. 2014. Evolution of online user behavior during a social upheaval. In *Proceedings of the 2014 ACM conference on Web science*. 81–90.

[48] Wikipedia. 2021. News media in the United States. *Wikipedia* (Feb 2021). https://en.wikipedia.org/w/index.php?title=News_media_in_the_United_States&%3Boldid=999240525