Political Activism and Technology

Alaa Daffalla and Alexandru G. Bardas

Abstract Activism, especially political activism, has been a driving force in changes throughout history. The ubiquity of smartphones and social media has significantly changed the landscape in terms of the tools that activists use and the extent of the legal and infrastructural power that nation states have over activists. For instance, political activists denouncing and fighting against oppressive regimes incorporate technology in their daily activities. They are using it to share information, mobilize and also organize their opposition movements. Meanwhile, their adversary can control and monitor the telecommunication infrastructure, aim to infiltrate their groups, arrest, or otherwise forcibly discourage them. In this chapter we shed light on the evolving defensive technology landscape that is enabling political activism in the modern era and the threat models behind it. It is vital for the technology community to understand political and societal contexts and how technology both enables and restricts various population groups as well as how it endangers and keeps them safe.

1 Activism and Technology Use

Activism is usually viewed through a number of different lenses, but a more general approach to activism involves actions taken by a group of people to achieve social, political, or environmental change [1]. The most known form of activism has been political activism but other forms of activism also emerged throughout the past decade. These other forms include: health activism [2, 3, 4], feminist movements [5], and climate change activism [6] among others.

Alaa Daffalla
Cornell University & Cornell Tech, New York City (NY) USA, e-mail: alaadaffalla@cs.cornell.edu

Alexandru G. Bardas
University of Kansas, Lawrence (KS) USA, e-mail: alexbardas@ku.edu

Various research works have examined technology use in different activism contexts. For example: in their work on health activism, Parker et al. [2] built Community Mosaic, a tool that allows users to share eating habits in an effort to advocate for behavior change. On the other hand, Consolvo et al. [3] designed a mobile application that encourages physical activity by sharing steps count with friends. In feminist activism Dimond et al. [5] discussed using technology intervention in the form of mobile applications and a blogging platform to prevent harassment and support activists when working with a social justice organization. The authors conclude that using technology for activism achieved a net positive outcome for the work of the organization. Fiesler et al. [7] also studied feminist human computer interaction (HCI) and incorporating feminist values into the design of systems. Furthermore, climate activism has recently emerged as a form of activism to advocate for and spread awareness about climate change. In specific, Hautea et al. [6] study the affordances and technical features of TikTok to see how creator's harness the platform for climate-change-related conversations.

The most studied form of activism in the modern technological literature is political activism [8, 9, 10, 11, 12] and it will be the main focus of this chapter. Along the lines of political activism, Tadic et al. [8] studied Information and Communication Technology (ICT) use by activists in Bosnia and Herzegovina and likened it to the ICT use by non-profit organizations. They looked into the activists' ICT training and knowledge sources and concluded that enabling security, privacy, and anonymity remain the biggest hurdle that activists face. Additionally, Gaw et al. [9] examined how professional activists decide when to use encrypted email. Other groups have studied technology during political events, e.g., protesters during the Arab Spring [10, 11, 12], and by political refugees or other persecuted populations [13, 14, 15, 16, 17, 18]. Finally, in a series of studies on how to design technology solutions for activists and grassroots movements, Hirsch provided an analysis of contestational design processes, grounding their findings on the importance of considering politics a significant factor in technology design decisions [19].

Even though political activism has been a significant driving force in geopolitical changes throughout history, the ubiquity of smartphones and social media has changed the landscape in terms of the tools that activists use and the extent of the legal and infrastructural power that nation states have over activists [26].

Activists denouncing and fighting against oppressive regimes incorporate technology in their daily activities, using it to share information, mobilize and also organize their opposition activities [22]. At the same time, their adversary can aim to infiltrate their groups, arrest, or otherwise forcibly discourage them. The duration of a political activism movement often varies and depends on the goals of the movement but also other different factors. For example, some movements last for years [20, 21] while others only last for a few months usually quelled by governments or other state actors [20]. A political revolution can be viewed as a prolonged and

dramatic culmination of activism efforts and puts technology used by activists under extreme pressure because it may not be designed for those directly colliding with a nation-state adversary. Therefore, it is important to consider that while technology can protect and support them, it can also expose them to risk.

Hence, an ever changing landscape of an activism movement is often accompanied with a change in threat models and defensive technology use of the actors involved. As researchers, we think it might not be possible to study the capabilities of a nation state adversary to their full extent but we believe it is important to explore the dynamics of political activism through the lens of security and privacy research. Furthermore, there has been little work in the literature examining the defensive practices of political activists from a technical and human-centered approach. For example, Maia et al. [23] analyzed the security and privacy advice contained in safety guides given to Black Lives Matter (BLM) protesters. They created different classes of guidelines based on content: advice related to smartphone confiscation, communications, smartphone networks, and information/photo sharing. They followed the classification of advice with a survey to understand how well activists or protesters understood and followed these guidelines. Additionally, some research has also focused on the practices of the Hong Kong protesters, particularly as it relates to secure messaging [24] or the vulnerabilities of tools used in protest settings [25].

In this chapter we shed light on the evolving defensive technology landscape that is enabling political activism in the modern era and the threat models behind it. The findings in this work are synthesized from previous studies on Sudanese political activists during the 2018-2019 political revolution in Sudan e.g., [22], [26].

2 Threat Models and the Developing Technical-Defensive Landscape

Domestic and international political outlooks have fundamentally altered how people experience technology by establishing what technology is available to them (e.g., through sanctions and censorship) and which privacy features match their threat model. The legal right to privacy can be defined in various ways and the practices law enforcement follow are decisive in building technology users' threat models [26].

The 2018–2019 Sudanese revolution can be viewed as a case study where activists developed their threat models based on evolving political, social, and technological factors [22]. In 2018, due to the dire internal economic situation, a series of protests erupted and led to a revolution. Throughout the different phases of this revolution (Figure 1 pictures a summary timeline of the events), protesters were targeted by a number of state actors, including the police, the security services, the military, and a special division of the armed forces.

International sanctions on Sudan meant that smartphone users in Sudan did not have access to all apps and app features, including the entire Apple App store, and paid apps and features in the Google Play store [27]. After designating Sudan a sponsor of state terrorism, the United States imposed the first major economic

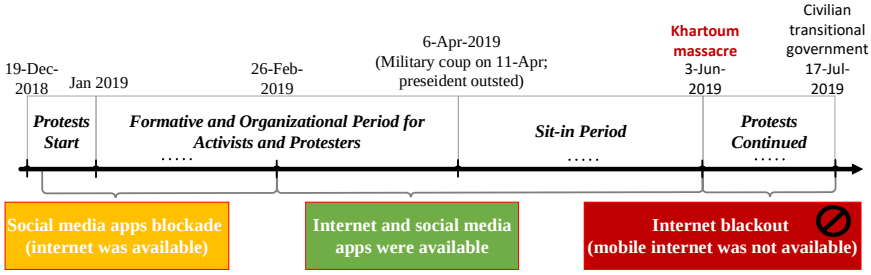

Fig. 1 Summary timeline of events and the impact on the availability of technology during the Sudanese 2018 - 2019 revolution.

sanctions on Sudan in 1996. The sanctions were partially lifted in 2015, giving Sudanese users access to unpaid apps and features in the Google Play store; however, paid apps and features in the Google Play store as well as the entire Apple App store were unavailable until December 2020, when the remaining U.S. sanctions were lifted. These restrictions shaped Sudanese activists' and protesters' capabilities and technology use. Thus, international politics can make it challenging to create security and privacy recommendations that fit multiple at-risk user groups as different groups have fundamentally different access to applications and apps features.

Based on the accounts of participants interviewed as part of [22, 26], using virtual private networks (VPN) was one way to circumvent the sanctions; however, it was often not a reliable option. Thus, it was more common that a store selling smartphones was using their store's (Apple) ID to pre-install apps on the iPhones sold to their customers. It is worth noting that sharing Apple IDs may impede privacy while a download from a nonofficial app store raises questions of app authenticity.

Additionally, people in Sudan couldn't directly pay for apps or app features due to economic sanctions, so apps with paid security or privacy features, or security and privacy-focused apps that are not free, were not easily accessible. The sanctions also meant that Sudanese domestic phone numbers were not accepted as a second factor of authentication (2FA) because in Sudan, Twitter did not employ verification for Sudanese numbers. Adding a foreign phone number to Twitter or WhatsApp accounts instead of a Sudanese phone number was a common practice. It was usually achieved in various ways, from using a foreign subscriber identification module (SIM) card on roaming to registering a temporary U.S. phone number online or asking friends overseas to validate accounts.

All these approaches encompassed a cost. For instance, although using a foreign SIM card made Sudanese activists and protesters feel safer because they believed the Sudanese government could not intercept their texts, this strategy may not have provided any privacy guarantees against interception or after-the-fact-reading for an adversary that has access to the telecommunications infrastructure. On the other hand, when creating the temporary U.S. numbers online through various web pages, activists were assuming that this would provide privacy by not going through the Sudanese telephone network, but they were fully relying on the security of the app

provider. Lastly, asking their friends and family overseas to verify their Twitter accounts by using foreign legitimate numbers provided the security of having 2FA not go through Sudan but required waiting for a message from someone who might be many time zones away when using 2FA (e.g., GMT-8 versus GMT+2).

2.1 Shaping Threat Models through the Technical Capabilities of Political Allies and Enemies

Activists' perceptions of the technical capabilities of foreign governments that supported the contested Sudanese regime, such as Saudi Arabia and the United Arab Emirates, were a driving factor in some participants' threat models. Some activists assumed that the Sudanese government could have the same access to information from social media companies as wealthier countries by purchasing such information from platforms such as Facebook [22].

The activists mistrust in Sudan's nation-state supporters extended to the foreign SIM cards they were using. As noted in [26], one activist believed that the Saudi government could acquire specific user data on behalf of the Sudanese regime through monetary influence and that they would pay Twitter to extract information about Sudanese users who had Saudi SIM cards. All this was assumed because entities close to the Saudi government own Twitter shares [30]. Thus, safe and roaming-enabled SIM cards were considered those associated with telecommunication companies from Europe or the United States.

An overall perception that users' privacy on social media could be breached with the financial means a government possess (especially, a rich government) led to a feeling of general uncertainty and mistrust. Despite this, protesters and activists continued to use popular social media platforms, such as Facebook, WhatsApp, due to their popularity and reach among the general population. Validating such beliefs can be a challenging endeavour. However, it is important to note that according to Facebook's public log of requests submitted by nation states, in the first half of 2019, there were 15 distinct requests by the Sudanese government, while in the second half of 2019, there were 52 requests. According to Facebook's data, the social media platform did not produce information in response to any of the requests [29].

2.2 The Power of the State to Compel Authentication

Users' technical practices are often shaped by their right to privacy as defined by local laws and practices. Although users in the United States may have legal protection against being compelled to give their passcode/password to law enforcement, aided by their smartphones' ability to force biometric authentication on demand or after a certain number of passcode/password attempts, Sudanese activists had no such protection and, thus, the same technical features did not provide the desired outcomes.

Sudanese authorities obtained arrestees' smartphone passcodes or biometrics to search their devices for anti-government activities and proof of identity, a major threat for all protesters. The threat of legal (or legally unquestioned) violence was always present throughout the Sudanese revolution. As stated in various accounts by Sudanese activists the threat of physical-device seizure was well-known [26]. Authorities would first look into the WhatsApp activity on the device followed by Facebook. After analyzing the latest posts they would conclude whether the owner of the device had a history of anti-goverment posts.

In recounting their arrest, an activist described that they were so confident in their defenses that they wrote down their passcode for the police. This confidence was not unwarranted: per their telling, they were detained for one week, all through which law enforcement had access to their phone. Because of the low-tech but meticulous defenses employed on the seized phone, law enforcement was not able to prove/infer that the arrested person was indeed an activist.

In anticipation of arrest and physical compromise of their phones, activists used a variety of low-tech defensive methods to hide or remove data. Thus, some of the activists manually deleted or hid information like contacts, WhatsApp or SMS messages, group chats, images, and social media accounts with anti-government or activist-related posts. Others formatted their phones entirely (reset to factory settings) while relying on backups. Some even planned to uninstall WhatsApp and Twitter and lean on a cloud backup if they were arrested. In this case activists usually had two SIM cards, with the second SIM providing plausible deniability. Messages were also regularly archived to a cloud instance. On the another hand, features such as iOS's Screen Time were leveraged in very creative ways. Screen Time is a feature intended to promote time management by hiding apps from the user outside a pre-configured schedule [31]. This feature was used to hide social media apps at certain key times – when at protests or when crossing the border.

One of the major strengths of these low-tech strategies is that they made it appear there was no information hidden or deleted. A complete lack of WhatsApp messages, for example, might be considered suspicious. However, participants who chose to delete information temporarily or permanently rather than conceal it on the device chose the cost of (temporary or permanent) data loss. Less commonly, participants used apps or operating system features specifically designed to conceal or delete information from their phones. Private Space on Huawei phones, which allows users to conceal certain information behind a secret PIN, and Twin Apps, which enables users to make a secret second copy of an app provided sufficient protection for some of the activists as they chose to not employ any other defensive strategies. In addition, some activists had apps such as "I'm Getting Arrested!" installed that would delete labeled data and send out a message to a list of numbers informing them that they got arrested. Telegram's self-deleting messages was also leveraged by some. Finally, protesters and activists who did not feel sufficiently protected by these available strategies chose to leave their smartphones at home and forgo any connection in favor of no liability.

2.3 Control Over the Telecommunication Infrastructure

The extent of a government's control and influence over the telecommunication infrastructure directly impacts the activists' threat model and defines their adoption of technology. For example, protesters and activists believed that the Sudanese government could monitor their communications through a combination of control over the telecommunications infrastructure, coercion of internet service providers, and technical exploitation. However, in order to enable this surveillance process in an environment dominated by pre-paid SIM cards, activists believed that the government needed to tie the real identity of a person to a specific phone number. An arrest would enable this mapping process. Thus, after getting arrested activists considered their phone number and sometimes even their smartphone device compromised and were acting accordingly by keeping a benign profile on the monitored phone number while pivoting to another device for activist-related activities.

Some activists were specific in differentiating between targeted and mass surveillance. Thus, they felt safe using mainstream apps and even regular text messages (SMS) if they sensed that they are not directly targeted by the government's monitoring capabilities. Moreover, there was a believe in "strength in numbers". If a large number of people are doing the same thing it would be impossible for the government to arrest everyone, especially if those people were simple protesters.

In addition to surveillance, censorship and blackout may complement the tool set of a powerful entity controlling the communication infrastructure. Such an entity with access to the communication infrastructure can try to interrupt and limit the spread of information. During the Sudanese revolution, government agencies were resetting passwords for Facebook accounts used to spread information about protests by triggering password resets and capturing the recovery SMSes. Furthermore, the government initially curtailed social media access for approximately ten weeks and a few months later they triggered a complete mobile data blackout after the Khartoum massacre on 3 June 2019 [32] (see Figure 1). On this date, armed government forces used gunfire and teargas to disperse a sit-in by protesters in front of the military headquarters in Khartoum killing and severely injuring hundreds of people. In the days following these events, mobile internet was completely blocked. As most of the people in Sudan do not have regular access to home internet, a mobile data blackout effectively serves as an internet blackout. Both, censorship and blackout, required people to find alternate communication solutions.

VPNs and the adoption of decentralized (peer-to- peer) networking apps, such as mesh networking chat apps, could serve as viable alternatives in such situations. As discussed in [26], activists encountered notable challenges that impeded adoption and reach. While the internet blackout was a period of (attempted) adoption of new apps and communication methods, many activists did not sufficiently fill their communication and confidentiality needs during this period. Some turned back to regular text messages, relying on strength in numbers, after attempting to adopt FireChat or Signal Offline Messaging, both mesh networking apps. Lack of group adoption and buggy applications, or usability issues accounted to the failure of pivoting to these new mediums. Some had difficulties with operating the app itself while other more

technical-proficient activists even tried to develop their own application. Since mesh networking chat applications suffer from the problem of group adoption, they are not useful until reaching a critical mass of users, and until then, users decide not to adopt them, preventing a critical mass [22].

Aside from the adoption challenge, another important aspect regarding mesh networking chat apps is the issue of download and setup without an internet connection. Unless a user can anticipate that they will not have internet, they will wait until they do not have internet, at which point they cannot download the app. Furthermore, although some mesh network apps use encryption, research work has revealed vulnerabilities in some of these apps such as Bridgify, a mesh networking app popular outside Sudan [33]. Mainstream apps are often developed with threat models that may prove too limited with respect to availability over a network controlled by an adversary, while apps specifically developed for use under an adversarial network (such as mesh networking apps) may grapple with adoption when internet is not available. These complexities emphasize the need to incorporate mesh networking and connection robustness into mainstream applications.

3 Societal Context and Technology Adoption

Social characteristics of a user population are critical factors in technology adoption. Activists in Sudan leveraged the strong existing social structure of the activism community and that of the general Sudanese society to spread security and privacy advice and adopt certain practices that helped them when contending with their adversary. A variety of societal characteristics of the Sudanese activist community contributed to the adoption of threat models and behaviors to mitigate misinformation within the activists' community and even the broader society. Institutional knowledge sharing, trust building, and external support manifested for the activist community turned into the ultimate social pillars that supported the activist movement.

3.1 Institutional Knowledge Sharing – Security and Privacy Advice

The activists' social structure facilitated the sharing of institutional knowledge in a mostly informal fashion. Social narratives about security and privacy were prevalent. Thus, a formal education or even an advertisement campaign for apps targeted at activists might be less successful than leveraging these social narratives. Although some of the activists were exposed to technical training, many relied on their friends and more experienced colleagues for security and technical advice through narratives and stories, confirming findings emphasized in multiple research works about security behavior adoption occurring socially [34, 35, 36].

Some of the so-called neighborhood committees during the Sudanese revolution had a resident security expert who taught their friends about apps such as Betternet (a

VPN application) and Private Space (an operating system feature on Huawei phones used to hide information). Furthermore, through their local neighborhood group, activists learned a few strategies to get access to the internet during the blackout. This involved breaching into the WiFi networks associated with landlines such as those powering automated teller machines or other government services/institutions.

Apps such as WiFi WPS Connect were leveraged to detect nearby networks. Next, activists made use of apps that were focused on either brute-forcing the WiFi-Protected Setup PIN, exploiting known vulnerabilities in older Wired Equivalent Privacy (WEP) networks, or on performing dictionary attacks on current WiFi Protected Access (WPA)/WPA2 networks. Dictionary-focused attacks make use of the initial handshake on a WPA/WPA2-personal WiFi network and try to consistently enter every word from a word list (a.k.a dictionary) to find the password for the protected WiFi network. Such word lists can range from a handful to millions of entries. Although activists were aware that cracking WiFi networks was illegal, they often had no other options to communicate with the outside world during the internet blackout. This underscores the importance of studying the security properties of such apps and their use by different groups, including activists.

3.2 Building Trust in a Mutating Group Surrounded by Uncertainty

Activist groups may be constantly changing, with members joining and leaving, resulting in a continuous need to build and maintain trust under uncertain circumstances filled with threats. Activists cannot trust everyone but they still have to trust other people so they can work together as a community. Often technology does not play a central role in building trust, an in-person meeting or a prior personal relationship are usually the prevalent means. While social media profiles can be used as part of a "background check," there was no one single technology that Sudanese activists relied on for trust building. This theme of nontechnical or low-tech approaches can be considered a strength because it decreases the technical attack surface, but could be vulnerable to other threats such as human intelligence infiltration. Thus, a boostrapping approach was often used for building in-person trust. New neighborhood committee members were mainly mutual acquaintances that were also vetted through the in-person campaigns to clean the streets after protests.

Similarly, activists relied on trusted contacts to add their own trusted contacts to the group or network in the cyberspace, or to gain trust for themselves and their online presence. Neighborhood committee's Twitter pages were often seeking to be a source of news and grow in size. An endorsement from such a verified account builds trust and increases the Twitter followers for the endorsed account substantially (e.g., in one case from 50 followers to nearly 4,000 within a few hours [22]). On the other hand, neighborhood committee social media accounts were often endorsed/verified by the Sudanese Professional Association, a trusted entity that played a central role in the 2018-2019 revolution.

All in all, activists relied on trusted contacts and networks to enable them to verify new members and even get news from a trusted, first-hand source. This network was sometimes multiple-layers deep so that it would be harder for an adversarial observer to trace through the entire network, specifically to map the original information source to a destination. For example, one activist built such a connection to verify news about deaths at protests: One (alleged) such death happened in another city in which the activist had a friend whose family was from that city, and that friend contacted a family member, who knew a doctor who worked at the hospital on the reported death date. Such social-technical-connected means were very common among activists to verify information and refute misinformation.

3.3 Support From Abroad

Generally, activist groups (despite their uniqueness) are not isolated and may be connected to a diaspora or other activist groups. These groups may be domestic or international. In case of the Sudanese activists, external support mainly enabled critical communication, helped with information verification and news dissemination during times when international journalists were not allowed in Sudan. Therefore, when studying activists one must consider the wider network of support that is involved, and how that network supports and influences the target activist group.

The Sudanese diaspora organized a content-moderation team on social media that was monitoring and questioning suspicious online accounts. This content-moderation community became organic and attempted to automate the process of combating misinformation online by building a platform that allowed the general public to upload information that they wanted to check. The verification was done using "Reddit-style" votes, up or down. However, not all votes had the same weight. There were specific voting weights assigned to verified voters, such as journalists, to determine the overall credibility of a piece of information/news. To encourage and support adoption, the platform collected only basic information to create the account and defend against automated trolls/bots.

Experienced activists in the diaspora also played an integral role in the flow of security and technical advice as they were exposed to a different set of tools that they were recommending to activists inside Sudan. Besides the diaspora, the activist social structure even extended to groups of other nationalities who may pass knowledge among a global network of activists. Per Daffalla et al. [26], the Signal messaging app was one of the tools recommended by external activists from other countries, specifically from Eastern Europe. While the different tools/apps and approaches can prove very useful in certain environments, they can also be ignored for no specific reason in environments where people are not used to them. This was the case for Signal during the 2018-2019 Sudanese revolution.

4 Conclusions – Needs and Technology

This chapter mainly focuses on one specific group of activists at a certain critical time, specifically during a revolution. While this chapter depicts events from the 2018-2019 revolution, and captures technology use by activists during this period we believe that the findings in this work can apply more broadly to activists, protesters, and other groups that contend with a nation state adversary and put technology use under extreme pressure. Nevertheless, there are many other political activist groups throughout the world in different political, societal, and technological contexts, which shape their use of technology based on the unique threats they are facing. For instance, political activists in Hong Kong contended with facial recognition by their adversary, and wore face masks until they were banned by the government [37]. Internet blackouts have been observed in Iran, Venezuela, and other countries after political protests, and censorship of various apps, websites, and technology is common throughout the world as well as international sanctions that restrict the availability of certain technologies [38, 39].

Contexts are diverse in nature and can create conflicting design needs among different populations. Thus, the major challenge that researchers, designers, and developers need to consider gravitates around the question of how to design tools that might provide affordances for one group, fitting its threat model and allowing it to protect itself, while not creating disaffordances and vulnerabilities for another at-risk group. fight against oppressive, discriminatory, and harmful forces. They may contend with a powerful adversary, which puts the technology they are using under a type of pressure that it may not have been designed to withstand. Therefore, activists often need to use technology in new and unexpected ways. Activism is only one example of how technology is not apolitical and design choices have physical and political consequences. For these reasons, it is important to study various population groups (especially at-risk ones) and follow their technological needs. As stated in [22], in these studies political, social, and technical factors should be carefully studied by considering aspects such as:

- The legal structure that defines the right to technical and physical privacy. Specifically, the power it provides to the governing entity and law enforcement.
- The extent of control and insight a powerful entity (such as a government) has into the telecommunications infrastructure and industry. Legal precedents, technical restrictions, and a history of censorship should all be taken into account.
- The technical capabilities of foreign powers that are allies or enemies with a certain nation. International sanctions and specifically what they restrict should be carefully analyzed.
- The baseline digital and security literacy for a group given their environment.
- Knowledge sharing mechanisms from social narratives to traditional platforms such as formal education and training.

All in all, it is vital for the technology community, in particular for the security and privacy community, to understand how technology both enables and restricts various population groups as well as how it endangers and keeps them safe.

References

1. Blomley, Nicholas K. “Activism and the academy.” Environment and planning D: Society and Space 12.4 (1994): 383-385.
2. Parker, A., Kantroo, V., Lee, H. R., Osornio, M., Sharma, M., Grinter, R. (2012, May). “Health promotion as activism: building community capacity to effect social change.” In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 99-108).
3. Consolvo, S., Everitt, K., Smith, I., Landay, J. A. (2006, April). “Design requirements for technologies that encourage physical activity.” In Proceedings of the SIGCHI conference on Human Factors in computing systems (pp. 457-466).
4. Grimes, A., Grinter, R. “Designing persuasion: Health technology for low-income African American communities.” International Conference on Persuasive Technology. Springer, Berlin, Heidelberg, 2007.
5. Dimond, J.P. “Feminist HCI for real: Designing technology in support of a social movement.” Georgia Institute of Technology, 2012.
6. Hautea, S., Parks, P., Takahashi, B., Zeng, J. (2021) “Showing they care (or don’t): Affective publics and ambivalent climate activism on TikTok.” Social Media+Society, 7(2), 20563051211012344.
7. Fiesler, C., Morrison, S., Bruckman, A.S. “An archive of their own: A case study of feminist HCI and values in design.” Proceedings of the 2016 CHI conference on human factors in computing systems. 2016.
8. Tadic, B., Rohde, M., Wulf, V., Randall, D. (2016, May). “ICT use by prominent activists in Republika Srpska”. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (pp. 3364-3377).
9. Gaw, Shirley, Edward W. Felten, and Patricia Fernandez-Kelly. “Secrecy, flagging, and paranoia: adoption criteria in encrypted email.” Proceedings of the SIGCHI conference on human factors in computing systems. 2006.
10. Lotan, G., Graeff, E., Ananny, M., Gaffney, D., Pearce, I. (2011). “The Arab Spring| the revolutions were tweeted: Information flows during the 2011 Tunisian and Egyptian revolutions”. International journal of communication, 5, 31.
11. Howard, P. N., Duffy, A., Freelon, D., Hussain, M. M., Mari, W., Maziad, M. (2011). “Opening closed regimes: what was the role of social media during the Arab Spring?”. Available at SSRN 2595096.
12. Stepanova, Ekaterina. “The role of information communication technologies in the “Arab Spring”.” Ponars Eurasia 15.1 (2011): 1-6.
13. Simko, L., Lerner, A., Ibtasam, S., Roesner, F., Kohno, T. (2018, May). “Computer security and privacy for refugees in the United States”. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 409-423). IEEE.
14. Guberek, T., McDonald, A., Simioni, S., Mhaidli, A. H., Toyama, K., Schaub, F. (2018, April). “Keeping a low profile? Technology, risk and privacy among undocumented immigrants”. In Proceedings of the 2018 CHI conference on human factors in computing systems (pp. 1-15).
15. Dhoest, Alexander. “Digital (dis) connectivity in fraught contexts: The case of gay refugees in Belgium.” European Journal of Cultural Studies 23.5 (2020): 784-800.
16. Portillo, Oliver. “To Liberate and Lament: The Duality of Digital Culture and Chechnya’s Concentration Camps for Russian LGBT Citizens.” EXCLAMATION (June 2018) (2018).
17. Panzica, Martine. “A difficult line to walk: NGO and LGBTQ+ refugee experiences with information and communications technology (ICT) in Canada.” (2020).

18. Dekker, R., Engbersen, G., Klaver, J., Vonk, H. (2018). “Smart refugees: How Syrian asylum migrants use social media information in migration decision-making”. Social Media+ Society, 4(1), 2056305118764439.
19. Hirsch, Tad. “Feature Learning from activists: Lessons for designers.” Interactions 16.3 (2009): 31-33.
20. Buettner, Ricardo, and Katharina Buettner. “A systematic literature review of twitter research from a socio-political revolution perspective.” 2016 49th hawaii international conference on system sciences (hicss). IEEE, 2016.
21. Ansani, Andrea, and Vittorio Daniele. “About a revolution: The economic motivations of the Arab Spring.” International Journal of Development and Conflict 2.03 (2012): 1250013.
22. Daffalla*, A., Simko*, L., Kohno, T., Bardas, A.G., “Defensive Technology Use During the 2018-2019 Sudanese Revolution.” In IEEE Security&Privacy Magazine (Special Issue), vol. 20, no. 2, issn 1558-4046, pp. 40-48, March-April 2022.
23. Boyd, M. J., Sullivan Jr, J. L., Chetty, M., & Ur, B. (2021, May). Understanding the Security and Privacy Advice Given to Black Lives Matter Protesters. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (pp. 1-18).
24. Albrecht, M. R., Blasco, J., Jensen, R. B., & Mareková, L. (2021). Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong. In 30th USENIX Security Symposium (USENIX Security 21) (pp. 3363-3380).
25. Albrecht, M. R., Blasco, J., Jensen, R. B., & Mareková, L. (2021, May). Mesh messaging in large-scale protests: Breaking Bridgefy. In Cryptographers’ Track at the RSA Conference (pp. 375-398). Springer, Cham.
26. Daffalla*, A., Simko*, L., Kohno, T., Bardas, A.G., “Defensive Technology Use by Political Activists During the Sudanese Revolution.” In Proceedings of the 2021 IEEE Symposium on Security and Privacy (S&P), pp. 372-390 , May 2021.
27. U.S. Office of Foreign Assets Control, In: Sanctions Programs and Country Information. Available via the U.S. Department of the Treasury. “https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information” of subordinate document. Cited 26 Sep 2022
28. CNN, In: Russia is plundering gold in Sudan to boost Putin’s war effort in Ukraine. Available via the CNN World. “https://www.cnn.com/2022/07/29/africa/sudan-russia-gold-investigation-cmd-intl/index.html” of subordinate document. Cited 26 Sep 2022
29. Facebook, In: Government Requests for User Data. Available via the Facebook Transparency Center. “https://govtrequests.facebook.com/government-data-requests/country/SD/jul-dec-2019” of subordinate document. Cited 27 Sep 2022
30. Computer World, In: Arab prince buys Twitter stake; recoils from Arab Spring. Available via U.S. Computer World. “https://www.computerworld.com/article/2471759/arab-prince-buys-twitter-stake–recoils-from-arab-spring.html” of subordinate document. Cited 27 Sep 2022
31. Apple, In: Use Screen Time on your iPhone, iPad, or iPod touch. Available via Apple Support. “https://support.apple.com/en-us/HT208982” of subordinate document. Cited 27 Sep 2022
32. The New York Times, In: 100 Killed in Sudan and Dozens of Bodies Are Pulled From Nile, Opposition Says. Available via The New York Time Africa. “https://www.nytimes.com/2019/06/04/world/africa/sudan-war-facts-history.html” of subordinate document. Cited 27 Sep 2022
33. The New York Times, In: Mesh Messaging in Large-scale Protests: Breaking Bridgefy. Available via The New York Time Africa. “https://martinralbrecht.files.wordpress.com/2020/08/bridgefy-abridged.pdf” of subordinate document. Cited 27 Sep 2022

34. Das, S., Kramer, A.D.I., Dabbish, L.A., Hong, J.I., “The Role of Social Influence in Security Feature Adoption”, In Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work &; Social Computing, pp. 1416–1426, February 2015.
35. Wash, R., “Folk Models of Home Computer Security,” In Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS), July 2021.
36. Rader, E., Wash, R., Brooks, B., “Stories as Informal Lessons about Security,” In Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS), July 2012.
37. Mozur P., “In Hong Kong Protests, Faces Become Weapons,” https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html, Cited 27 Sep 2022
38. Newman, L.H., “How the Iranian Government Shut Off the Internet,” https://www.wired.com/story/iran-internet-shutoff/, Cited 27 Sep 2022
39. Thorbecke, C., In: How the Iranian Government Shut Off the Internet. Available via CNN Business. https://www.cnn.com/2022/09/24/tech/iran-internet-blackout/index.html, Cited 27 Sep 2022